

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«До захисту допущено»

Завідувач кафедри

_____ Л.О. Уривський

«__» _____ 20__ р.

Дипломна робота

на здобуття ступеня бакалавра

**з напрямку підготовки 6.050903 Телекомунікації
(172 Телекомунікації та радіотехніка)**

**на тему: «Протоколи і технології передавання інформації для мереж
Інтернету речей»**

Виконав:

студент IV курсу, групи ТС-51
Шевчук Антон Олександрович

Керівник:

к.т.н., доцент
Мошинська Аліна Валентинівна

Рецензент:

старший викладач
Прищепа Тетяна Олексіївна

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.

Студент (-ка) _____

Київ – 2019 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – перший (бакалаврський)

Напрямок підготовки – 6.050903 «Телекомунікації» (172 Телекомунікації та радіотехніка)

Програма професійного спрямування – «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Л.О. Уривський

«___» _____ 20__ р.

ЗАВДАННЯ

на дипломну роботу студенту

Шевчуку Антону Олександровичу

1. Тема роботи «Протоколи і технології передавання інформації для мереж Інтернету речей», керівник роботи Мошинська Аліна Валентинівна, к.т.н., доцент, затверджені наказом по університету від «___» _____ 20__ р. № _____

2. Термін подання студентом роботи _____

3. Вихідні дані до роботи: інформаційні матеріали про технології та протоколи передачі інформації в мережах IoT. Структурований план порядку розробки матеріалів дипломної роботи.

4. Зміст роботи

Здійснити огляд архітектури, еталонної моделі та принципу дії Інтернету речей. Проаналізувати переваги та недоліки IoT. Здійснити огляд технологій та протоколів передачі повідомлень та даних на довгі та короткі відстані в IoT та провести порівняльний аналіз характеристик. Здійснити огляд

проблематики передачі повідомлень в мережі IoT. Проаналізувати сучасний стан та перспективи розвитку технологій передачі даних в мережі IoT.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

- 1) Загальна характеристика дипломної роботи;
 - 2) Архітектура мережі Інтернету речей;
 - 3) Порівняльний аналіз характеристик технологій та протоколів передачі даних на довгій відстані;
 - 4) Порівняльний аналіз характеристик технологій та протоколів передачі даних на короткій відстані;
 - 5) Порівняльний аналіз характеристик протоколів передачі повідомлень;
 - 6) Висновки.
6. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Розробка, оформлення, узгодження та затвердження технічного завдання на роботу. Аналітичний огляд інформаційних матеріалів. Підбір та опрацювання необхідної науково-технічної літератури.	1.01.2019-31.01.2019	Викон.
2	Огляд архітектури, еталонної моделі та принципу дії Інтернету речей. Аналіз переваг та недоліків IoT.	1.02.2019-17.02.2019	Викон.
3	Огляд технологій та протоколів передачі даних на довгій відстані в IoT та проведення порівняльної характеристики основних функцій.	18.02.2019-28.02.2019	Викон.
4	Огляд технологій та протоколів передачі даних на довгій відстані в IoT та проведення порівняльної характеристики основних функцій.	1.03.2019-17.04.2019	Викон.
5	Огляд проблематики передачі повідомлень в мережі IoT. Огляд протоколів передачі повідомлень та проведення їх порівняльної характеристики.	17.04.2019-16.05.2019	Викон.
6	Аналіз сучасного стану та перспектив розвитку технологій передачі даних в мережі IoT.	17.05.2019-31.05.2019	Викон.
7	Узагальнення, підготовка підсумкового звіту. Подання роботи до приймання, та її захист.	1.06.2019-18.06.2019	Викон.

Студент

Шевчук А.О.

Керівник роботи

Мошинська А.В.

РЕФЕРАТ

Текстова частина дипломної роботи: 76 с., 25 рис., 4 табл., 38 джерел.

Мета роботи – аналіз архітектури, моделі, та принципу дії Internet of Things. Здійснення порівняльного аналізу характеристик протоколів та технологій передачі даних на довгі та короткі відстані та протоколів передачі повідомлень. Аналіз сучасного стану та перспектив розвитку технологій передачі даних в Україні.

Дана робота складається з трьох основних частин:

В першій частині проведено аналіз архітектури та еталонної моделі Інтернету речей та їх складових елементів. Досліджено принцип роботи, а також розглянуто переваги та недоліки Інтернету речей.

В другій частині описуються технології передачі даних на довгі та короткі відстані в IoT, а також протоколи для передачі повідомлень. Проведений порівняльний аналіз базових характеристик протоколів та технологій передачі даних та повідомлень.

В третій частині було проведено аналіз сучасного стану та перспектив розвитку технологій передачі даних IoT в Україні.

Ключові слова: IoT, мережа, датчик, рівень, протокол, передача даних.

ABSTRACT

The text part of the diploma: 76 pages, 25 fig., 4 tab., 38 sources.

The purpose of this work is analyzing architecture, model and working principle of Internet of Things. Performing comparative analysis of the characteristics of data transmission protocols and technologies on long and short distances and protocols for transmission messages. Analysis of the current condition and development prospects data transmission technologies in Ukraine.

This work consists of three main parts:

In the first part are analysed architecture and reference model Internet of things and their components. Investigated working principle and also advantages and disadvantages Internet of things.

In the second part are described data transmission technologies on long and short distances in IoT and also protocols for transmission of messages. Implemented comparative analysis basic characteristics of protocols and data transmission technologies and messages.

In the third part are carried out analysis current condition and development prospects data transmission technologies IoT in Ukraine.

Key words: IoT, network, sensor, level, protocol, data transmission.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ.....	10
ВСТУП.....	12
1 МЕТОДОЛОГІЧНІ АСПЕКТИ РОБОТИ МЕРЕЖІ ІОТ.....	14
1.1 Базові визначення в мережі ІоТ.....	14
1.2 Архітектура ІоТ.....	14
1.2.1 Рівень датчиків.....	15
1.2.2 Мережевий рівень.....	17
1.2.3 Рівень обробки даних.....	17
1.2.4 Рівень додатків.....	17
1.3 Принцип роботи ІоТ.....	18
1.3.1 Зчитування інформації за допомогою датчиків.....	18
1.3.2 Передача даних від датчиків до хмарних сховищ.....	19
1.3.3 Обробка даних отриманих за допомогою датчиків...	19
1.3.4 Передача даних на інтерфейс користувача.....	20
1.4 Еталонна модель ІоТ.....	20
1.4.1 Прикладний рівень.....	21
1.4.2 Рівень підтримки послуг та додатків.....	22
1.4.3 Мережевий рівень.....	22
1.4.4 Рівень пристроїв.....	23
1.4.5 Можливості управління.....	24
1.4.6 Можливості забезпечення безпеки.....	25
1.5 Переваги ІоТ.....	25
1.6 Недоліки ІоТ.....	27
1.7 Висновки до розділу 1.....	29

					НТУУ 1068-с 10.ТС-51.2019.ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Протоколи і технології передавання інформації для мереж Інтернету речей	Лім.	Арк.	Акрушіє
Розроб.		Шевчук А.О.					7	77
Перевір.		Мошинська А.В.				ІТС		
Реценз.		Прищепя Т.О.						
Н. Контр.		Новіков В.І.						
Затверд.		Уризський Л.О.						

2 ОГЛЯД ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОТОКОЛІВ ТА ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ ТА ПОВІДОМЛЕНЬ В МЕРЕЖАХ ІОТ	30
2.1 Технології та протоколи передачі даних на довгі відстані в ІоТ мережах	30
2.1.1 LoRaWAN	30
2.1.2 SigFox	34
2.1.3 NB-IoT	36
2.1.4 Weightless-P	39
2.1.5 Порівняльна характеристика технологій передачі даних на довгі відстані в мережі ІоТ	41
2.2 Технології та протоколи передачі даних на короткі відстані в ІоТ мережах	41
2.2.1 Z-Wave	41
2.2.2 NFC	42
2.2.3 RFID	44
2.2.4 Bluetooth Low Energy	46
2.2.5 Wi-Fi HaLow	48
2.2.6 Порівняльна характеристика технологій та протоколів передачі даних на короткі відстані в ІоТ	50
2.3 Протоколи для передачі повідомлень в ІоТ	50
2.3.1 Проблематика передачі повідомлень в мережі ІоТ	50
2.3.2 Базова топологія, яка використовується для передачі повідомлень в ІоТ	51
2.3.3 DDS	52
2.3.4 XMPP	54
2.3.5 CoAP	55
2.3.6 MQTT	56
2.3.7 STOMP	58

2.3.8 SOAP.....	59
2.3.9 Порівняльна характеристика протоків передачі повідомлень.....	61
2.4 Висновки до розділу 2.....	62
3 СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ ІОТ В УКРАЇНІ.....	63
3.1 Сучасний стан технологій передачі даних в Україні.....	63
3.2 Перспективи розвитку технологій передачі даних в Україні.....	64
3.2.1 Сектор медицини.....	66
3.2.2 Безпілотні авто та кватдрокоптери.....	67
3.2.3 Розумні будинки.....	69
3.3 Висновки до розділу 3	70
ВИСНОВКИ.....	71
ПЕРЕЛІК ПОСИЛАНЬ.....	73

ПЕРЕЛІК СКОРОЧЕНЬ

BLE	Bluetooth Low Energy – Bluetooth з низьким енергоспоживанням
CoAP	Constrained Application Protocol – протокол обмеженого користування
DDS	Data Distribution Service – протокол, який передає дані між різними пристроями
HTTP	HyperText Transfer Protocol – протокол передачі гіпер-текстових документів
IoT	Internet of Things – Інтернет речей
LoRa	Long Rang – назва протоколу фізичного рівню та технології, які використовують метод модуляції оснований на техніці розширення спектру
LoRaWAN	Long Rang Wide Area Network – протокол канального рівня, що базується на технології LoRa
LPWAN	Low Power Wide Area Network – енергоефективна мережа дальнього радіусу дії
LTE	Long-Term Evolution – назва мобільного протоколу передачі даних четвертого покоління
M2M	Machine-to-Machine – технологія машино-машинної взаємодії, що дозволяє передавати дані між різними пристроями.
MQTT	Message Queue Telemetry Transport – спрощений транспортний протокол, який орієнтований на обмін повідомленнями між пристроями по принципу «видавець-передплатник»
NB-IoT	Narrow Band Internet of Things – стандарт стільникового зв'язку, який використовується для пристроїв телеметрії з низьким об'ємом обміну даних

NFC	Near Field Communication – технологія бездротового високочастотного зв'язку малого радіусу дії
NGN	Next Generation Network – це мультисервісна мережа зв'язку, яка підтримує інтеграцію послуг та базується на IP-мережі
QoS	Quality of Service – якість обслуговування
RFID	Radio Frequency Identification – радіочастотна ідентифікація
SOAP	Simple Object Access Protocol – протокол обміну структурованими повідомленнями в розподілених обчислювальних системах, базується на форматі XML
STOMP	Simple Text-Oriented Messaging Protocol – простий протокол обміну повідомленнями
TCP	Transmission Control Protocol – протокол управління передачею
XML	Extensible Markup Language – розширювана мова розмітки
XMPP	Extensible Messaging and Presence Protocol – протокол для обміну миттєвими повідомленнями та інформацією про присутність

ВСТУП

В наш час Інтернет речей — це зовсім новий етап розвитку Інтернету.[1] З розвитком комп'ютерних технологій почали розширювати спроможність аналізу, передачі, збору та розподілу даних. Після цього кожна людина може трансформувати ці дані в структуровану інформацію, а потім в знання.

Інтернет речей (IoT) з'єднує кожен об'єкт нашого життя з Інтернетом. Це допомагає нам більш якісно виконувати збір, аналіз та отримання даних, які декілька років тому були недоступними для звичайної людини.

Концепція IoT дозволяє не тільки з'єднувати речі, що пов'язані з благами матеріального світу за допомогою Інтернету для можливості обміну інформацією між ними, але й дає можливість розвивати способи по аналізу, накопиченню та структуруванню отриманої інформації.

Під поняттям Інтернету речей усвідомлюють не тільки велику кількість різноименних датчиків, приладів, які об'єднані за допомогою безпроводових та проводових технологій та протоколів передачі даних підключених до Інтернету, але й досить тісну взаємодію між віртуальними та реальними світами, в яких діалог відбувається між пристроями та людиною.

По факту, Інтернет речей — це глобальна мережа речей-приладів, які під впливом деякої програми приймають певні рішення з приводу тих чи інших дій, що виконуються без участі людини.[3]

Крім звичайних приладів, якими ми користуємося кожного дня (конвеєрна стрічка, чайник, годинник, пилосос), у цій мережі повинні бути залучені різного роду датчики (ваги, вібрації, температури та ін.). Тобто пристрої, що будуть зберігати зібрану інформацію і пристрої, які будуть керувати всіма цими процесами. Схематичне зображення пристроїв, які можуть бути об'єднані в мережі IoT зображено на рис. 1.

1 МЕТОДОЛОГІЧНІ АСПЕКТИ РОБОТИ МЕРЕЖІ IoT

1.1 Базові визначення в мережі IoT

Мережа наступного покоління (NGN) – це мережа з пакетною комутацією, придатна до надання послуг електрозв'язку та для використання декількох широкосмугових технологій транспортування з ввімкненою функцією якості обслуговування (QoS), в якій зв'язані з обслуговуванням функції не залежать від використаних технологій, що забезпечують транспортування.[4]

Пристрій – обладнання, яке володіє обов'язковими можливостями зв'язку та додатковими можливостями такими, як: вимірювання, спрацювання, а також введення, зберігання та обробку даних.

Інтернет речей (IoT) – це глобальна інфраструктура для інформаційного суспільства, котра забезпечує можливість надання більш важких послуг шляхом з'єднання один з одним (фізичних та віртуальних) речей на основі наявних функціонально сумісних інформаційно-комунікаційних технологій.

1.2 Архітектура IoT

Архітектура IoT пристроїв складається з чотирьох рівнів: рівень датчиків, мережевий рівень, рівень обробки даних та прикладний рівень (див. рисунок 1.1). Більш детальне описання кожного рівню архітектури наведено нижче.

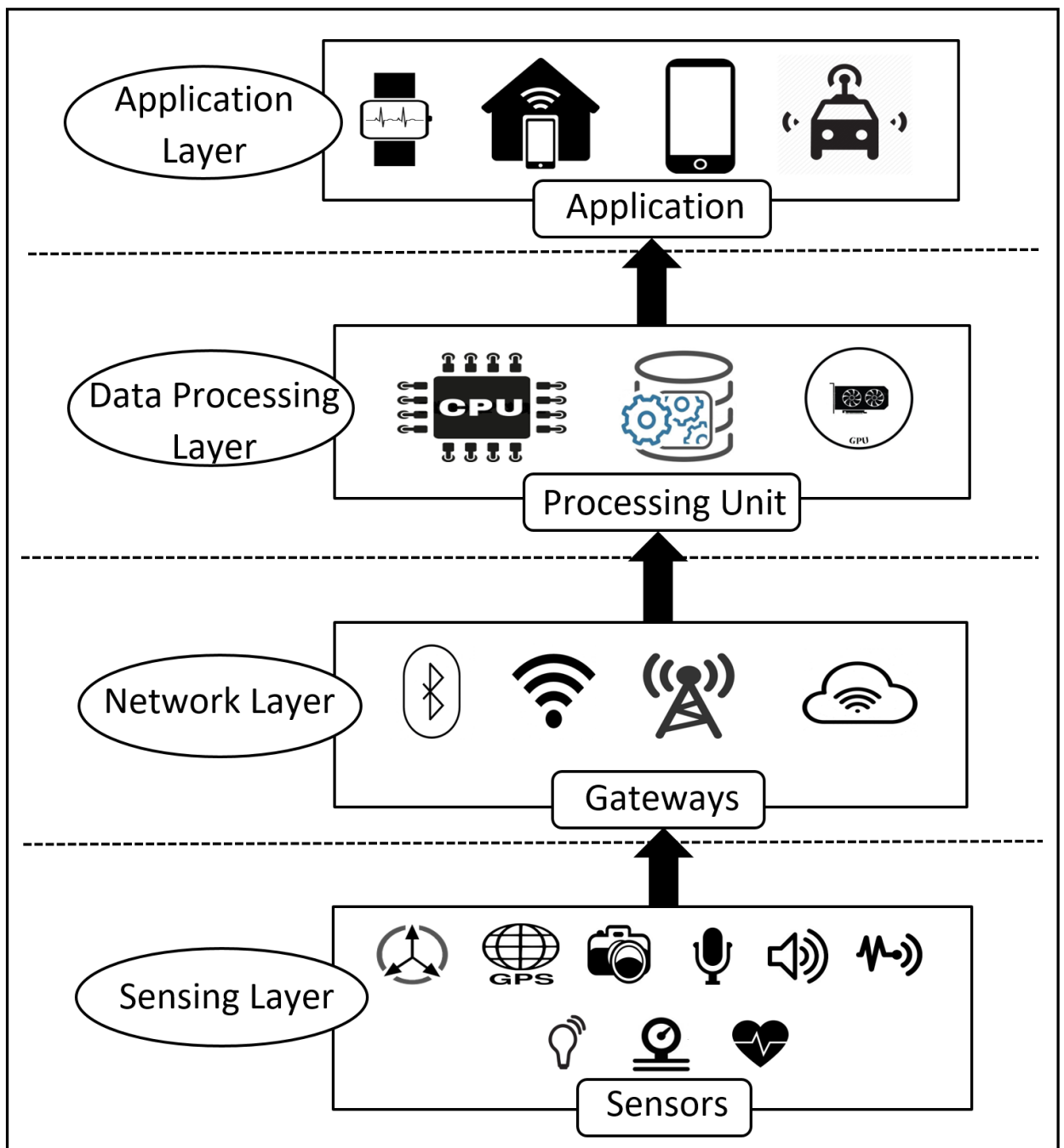


Рисунок 1.1 Архітектура мережі IoT[5]

1.2.1 Рівень датчиків

Головна мета рівня датчиків – ідентифікація різних явищ навколишнього середовища за допомогою периферійних пристроїв та отримання даних з реального світу.[5] Цей рівень складається з декількох видів датчиків. Використання великої кількості датчиків є однією з найважливіших функцій IoT пристроїв. Датчики в IoT пристроях зазвичай

інтегруються за допомогою концентратора датчиків. Концентратор датчиків є головною точкою з'єднання для кількох датчиків. Він акумулює та передає дані з датчиків до блоку обробки даних в пристрої. Концентратор датчиків використовує декілька транспортних механізмів таких, як (Inter-Integrated Circuit (I2C) чи Serial Peripheral Interface (SPI)) для передачі даних між датчиками та додатками. Ці транспортні механізми залежать від IoT пристроїв. Вони створюють канал зв'язку між датчиками та додатками збору даних з датчиків.

Датчики в IoT пристроях можуть бути класифіковані на 3 широкі категорії:

- Датчики руху, які вимірюють зміни в русі, а також орієнтацію пристроїв. Є два типи рухів, які можна спостерігати за допомогою датчику цього пристрою: лінійний та кутовий рух. Лінійний рух відноситься до лінійного переміщення пристрою IoT, в той час як кутовий рух відноситься до обертового переміщення пристрою.

- Датчики навколишнього середовища до них відносяться такі пристрої, як датчики світла, датчики тиску та інші, які вбудовані в IoT пристрої реагують на зміни в параметрах навколишнього середовища за допомогою периферійних пристроїв. Основною метою використання цих датчиків в IoT пристроях є допомога пристроям приймати автономні рішення відповідно до змін в периферійних пристроях. Наприклад, датчики навколишнього середовища використовуються в більшості додатків для спрощення життя користувачів (розумні замки, система домашньої автоматизації, розумне освітлення та ін.).

- Датчики місцеперебування пристроїв IoT взаємодіють з фізичним місцеперебуванням та розташуванням самого пристрою. Найбільш поширеними датчиками місцеперебування, що використовуються в IoT є магнітні датчики та Global Position System (GPS) датчики. Магнітні датчики використовуються, як цифрові компаси та допомагають фіксувати орієнтацію

дисплею пристрою. GPS датчики використовуються для навігаційних цілей в IoT пристроях.

1.2.2 Мережевий рівень

Мережевий рівень використовується, як комунікаційний канал для передачі даних, зібраних на рівні датчиків, до інших підключених пристроїв. В IoT пристроях, мережевий рівень реалізований для використання різноманітних комунікаційних технологій (наприклад, Z-Wave, LoRa, Wi-Fi, Bluetooth та ін.), що дозволяють передавати дані між різними пристроями всередині самої мережі.

1.2.3 Рівень обробки даних

Рівень обробки даних складається з головного блоку обробки даних IoT пристрою. Рівень обробки даних отримує зібрані дані на рівні датчиків та аналізує їх. Потім приймає рішення, що базуються на результаті аналізу. В деяких IoT пристроях (наприклад, смарт-годинник, розумний домашній концентратор та ін.), цей рівень також зберігає результати попередніх аналізованих даних для подальшої можливості використання цих даних. Також цей рівень може передавати результати обробки даних з одного підключеного пристрою на інший пристрій через мережевий рівень.

1.2.4 Рівень додатків

Рівень додатків презентує результати роботи рівню обробки даних за допомогою різного роду додатків IoT пристроїв. Рівень додатків є рівнем орієнтованим на користувачів, який виконує різні завдання для користувача. Існують різні IoT додатки, які включають розумний будинок, розумний транспорт тощо.

1.3 Принцип роботи IoT

На рис. 1.2 зображено принцип роботи найпростішої мережі IoT.

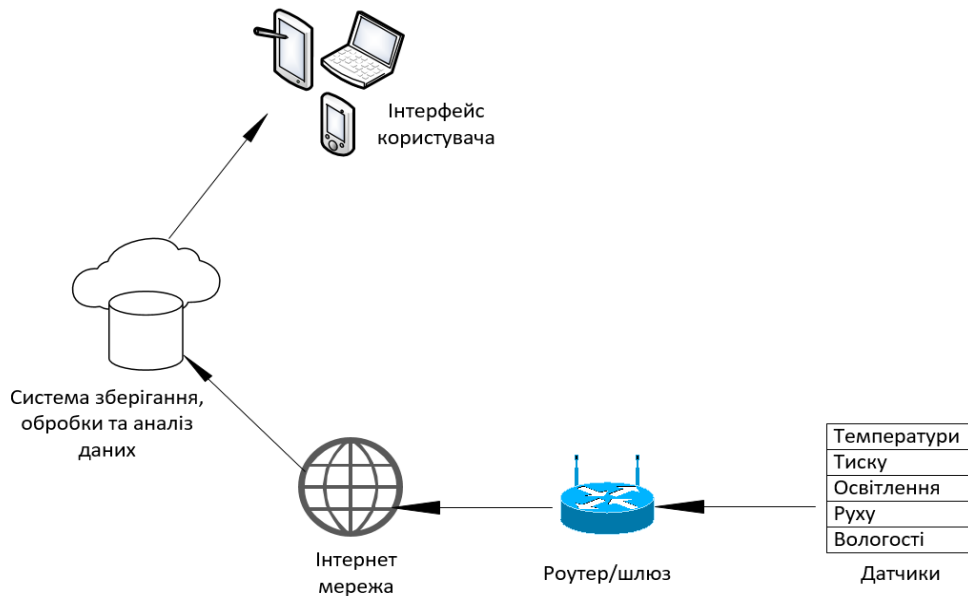


Рисунок 1.2 Принцип роботи IoT

Принцип роботи IoT об'єднує чотири різні етапи:

- Зчитування інформації за допомогою датчиків;
- Передача даних від датчиків до хмарних сховищ;
- Обробка даних отриманих за допомогою датчиків;
- Передача інформації на інтерфейс користувача.[6]

Нижче описано кожен з етапів більш детально.

1.3.1 Зчитування інформації за допомогою датчиків

По-перше, датчики або пристрої збирають дані зі свого оточення. Це може бути як простим процесом, таким як зчитування температури, або складним, як запис відео на камеру відеоспостереження.

Використовується на даному етапі також й пристрої, оскільки декілька датчиків можуть бути об'єднані разом або датчики можуть бути частиною пристрою, що робить більше, ніж просто аналіз даних. Наприклад, ваш телефон - це пристрій з кількома датчиками (камера, акселерометр, GPS тощо), але телефон не є лише датчиком.

На цьому кроці дані збираються з нашого оточення.

1.3.2 Передача даних від датчиків до хмарних сховищ

Датчики можуть бути підключені до хмари за допомогою різних методів, включаючи: стільникову мережу, супутникову мережу, Wi-Fi, Bluetooth, малопотужні широкосмугові мережі (LPWAN), або з'єднатися безпосередньо до Інтернету через Ethernet технологію.

Кожна опція має компроміс між споживанням енергії, діапазоном та пропускною здатністю. Вибір того чи іншого варіанту підключення зводиться до вибору конкретної області, де буде використовуватися Інтернет речей, але всі вони виконують одне і те ж завдання - передачу даних до хмари.

1.3.3 Обробка даних отриманих за допомогою датчиків

Після того, як дані потрапляють до хмари, програмне забезпечення виконує певну обробку даних.

Це може бути, наприклад, перевірка того, що зчитувана температура знаходиться в межах допустимого діапазону. Чи це може бути процесом обробки інформації, наприклад, використання комп'ютерного програмного забезпечення, яке здійснює ідентифікацію об'єктів, що знаходяться на відео (наприклад, злоумисників у вашому домі).

1.3.4 Передача інформації на інтерфейс користувача

На даному етапі відбувається передача корисної інформації кінцевому користувачу певним чином. Це може бути через сповіщення користувача (електронна пошта, текст, сповіщення тощо). Наприклад, текстове сповіщення, коли температура занадто висока в холодному сховищі компанії.

Крім того, користувач може мати інтерфейс, який дозволяє йому активно перевіряти систему. Наприклад, користувач може захотіти перевірити камери відеоспостереження в їхньому будинку через телефонну програму, або веб-сторінку.

Однак це не єдиний шлях. Залежно від програми IoT, користувач може також виконувати дії на відстані та впливати на систему. Наприклад, користувач може дистанційно регулювати температуру в холодному сховищі за допомогою програми на своєму телефоні.

А деякі дії виконуються автоматично. Замість того, щоб чекати, коли користувач налаштує температуру, система може зробити це автоматично за допомогою попередньо визначених правил. І замість того, щоб просто викликати вас, щоб попередити вас про зловмисника, система IoT також може автоматично повідомляти відповідні органи.

Система IoT складається з датчиків, які розмовляють з хмарою через певний тип зв'язку. Після того, як дані потрапляють у хмару, програмне забезпечення обробляє його, а потім може вирішити виконати певну дію, наприклад, надіслати попередження, або автоматично регулювати роботу датчика без потреби користувача.

1.4 Еталонна модель IoT

На рисунку 1.3 показана еталонна модель IoT, яка наведена в рекомендації Y.2060, вона складається з чотирьох основних рівнів, а також з двох додаткових рівнів: можливості управління та безпеки.

До основних рівнів належить:

- прикладний рівень;
- рівень підтримки послуг та додатків;
- мережевий рівень;
- рівень пристроїв.[4]

Нижче описано кожен з рівнів більш детально.

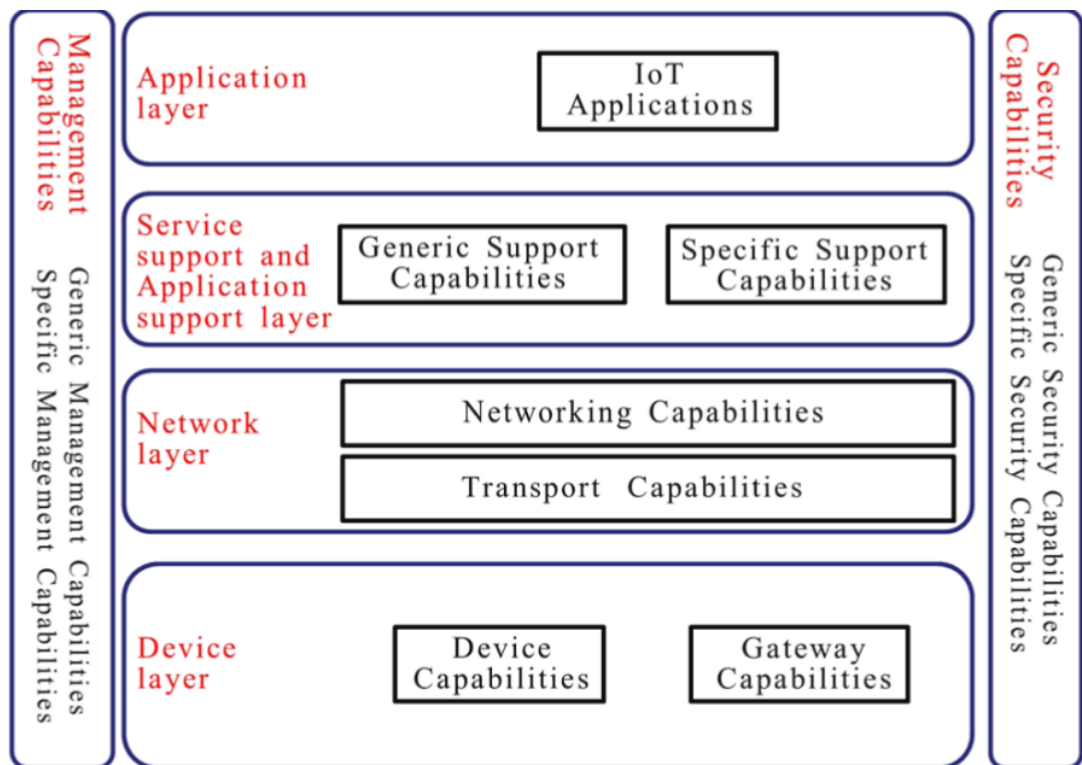


Рисунок 1.3 Еталонна модель IoT [4]

1.4.1 Прикладний рівень

Прикладний рівень в Рекомендації Y.2060 не розглядається.

1.4.2 Рівень підтримки послуг та додатків

Рівень підтримки послуг та додатків складається з наступних двох груп можливостей, таких як загальні можливості підтримки та спеціалізовані можливості підтримки:

- Загальні можливості підтримки - це можливості, які можуть використовуватися різними додатками такими як обробка та зберігання даних. Ці можливості можуть бути активовані за допомогою спеціалізованих можливостей підтримки, наприклад, для створення інших спеціалізованих можливостей підтримки;

- Спеціалізовані можливості підтримки - це конкретні можливості, які призначені для задоволення вимог різноманітних додатків. Насправді вони можуть складатися з ряду груп чітко визначених можливостей, для того щоб надавати різні функції підтримки різних програм IoT.

1.4.3 Мережевий рівень

Цей рівень складається з наступних двох типів можливостей:

- Можливості організації мереж: надає відповідні функції управління мережевим з'єднанням, такі як функції управління доступом та ресурсами транспортування, управління мобільністю або автентифікація, авторизація та облік (AAA).

- Можливості транспортування: призначені для надання з'єднання для транспортування інформації у вигляді даних, що відносяться до послуг і додатків IoT, а також транспортування інформації контролю та управління, що відносяться до IoT.

1.4.4 Рівень пристроїв

Можливості рівня пристроїв можна логічно розділити на два види можливостей:

- Можливості пристрою:

Можливості пристрою діляться в свою чергу на:

а) Пряму взаємодію з мережею зв'язку: пристрої здатні збирати та закачувати інформацію безпосередньо (тобто без використання можливостей шлюзу) в мережі зв'язку та можуть безпосередньо отримувати інформацію (наприклад, команди) із мережі зв'язку.

б) Непряму взаємодію мережі зв'язку: пристрої здатні отримувати та закачувати інформацію в мережі зв'язку непрямым чином, тобто за допомогою можливості шлюзу. На іншій стороні пристрою можуть не прямим чином отримувати інформацію (наприклад, команди) з мережі зв'язку.

Організація спеціальних мереж в ряді сценаріїв вимагає підвищену масштабованість та швидкого розгортання, пристрої можуть мати можливість будувати мережі довільним чином

в) Сплячий режим та пробудження: можливості пристроїв можуть підтримувати механізми "сну" і "пробудження" для економії енергії.

- Можливості шлюзу:

Можливості шлюзу включають, в тому числі:

а) Підтримку декількох інтерфейсів: на рівні пристроїв можливості шлюзу підтримують пристрої, сполучені з використанням різних дротових і бездротових технологій, таких як шина локальних мереж контролерів (CAN), Bluetooth, або Wi-Fi. На рівні мережевих можливостей шлюзу можуть обмінюватися даними з використанням різних технологій, таких як комутована телефонна мережа загального користування, мережі другого або третього покоління (2G або 3G), мережі на базі технології довгострокового розвитку (LTE), Ethernet або цифрові абонентські лінії (DSL).

б) Перетворення протоколу: існує дві ситуації в яких потрібні можливості шлюзу. Перша ситуація виникає тоді, коли для зв'язку на рівні пристроїв використовуються різні протоколи рівня пристроїв, наприклад, протоколу технологій Z-Wave, Bluetooth; друга ситуація виникає тоді, коли для зв'язку потребується і рівень пристроїв і мережевий рівень, використовуються різні технології, наприклад, протокол технології Z-Wave на рівні пристроїв і протокол технології 3G на мережевому рівні.

1.4.5 Можливості управління

За аналогією з традиційними засобами зв'язку, можливості управління IoT охоплює традиційні класи несправності, конфігурації обліку, показників роботи та безпеки (FCAPS), тобто управління несправностями, управління конфігурації, управління обліком, управління показниками роботи та управління безпекою.

Можливості управління IoT можуть бути поділені на категорії загальних можливостей управління і спеціалізованих можливостей управління.

Найважливіші загальні можливості управління в IoT включає:

- а) управління пристроями, наприклад дистанційне ввімкнення або вимкнення пристроїв, діагностика, оновлення прошивки та/або програмного забезпечення, управління робочим станом пристроїв;
- б) управління топологією локальної мережі;
- в) управління трафіком і перевантаженнями, наприклад виявлення умов перевантаженості мережі та реалізації резервування ресурсів для термінових та/або життєво важливих потоків трафіку.

Спеціалізовані можливості управління тісно пов'язана з вимогою додатків, наприклад вимогами по контролю лінії передачі електроенергії в розумній електромережі

1.4.6 Можливості забезпечення безпеки

Існує два види можливостей забезпечення безпеки: загальні можливості забезпечення безпеки та спеціалізовані можливості забезпечення безпеки.

- Загальні можливості забезпечення безпеки не залежить від додатків і включає:

а) на прикладному рівні: авторизацію, автентифікацію, захист конфіденційності та цілісності даних додатків, захист недоторканності приватного життя, аудит безпеки та антивірусну програму;

б) на мережевому рівні: авторизація, автентифікація, конфіденційність даних про використання та даних сигналізації, а також захист цілісності даних сигналізації;

в) на рівні пристроїв: автентифікація, авторизація, перевірку цілісності пристрою, управління доступом, захист конфіденційності і цілісності даних.

- Спеціалізовані можливості забезпечення безпеки тісно пов'язані з вимогами додатків, наприклад вимогам безпеки мобільних платежів.

1.5 Переваги IoT

До переваг в IoT відносять:

- Взаємозв'язок між приладами

IoT заохочує зв'язок між пристроями, також відомий як зв'язок між машинами (M2M). Через це фізичні пристрої можуть залишатися на зв'язку, а отже, загальна прозорість доступна з більшою якістю.[7-8]

- Автоматизація та управління

Завдяки фізичним об'єктам, підключеним і керованим цифровим способом і централізовано з бездротовою інфраструктурою, існує велика кількість автоматизації і контролю в роботах. Без втручання людини машини здатні спілкуватися один з одним, що призводить до швидшого і своєчасного обміну інформацією.

- Інформація

Очевидно, що більше інформації допомагає приймати кращі рішення. Незалежно від того, чи потрібні знання про те, що купувати в продуктовому магазині, або якщо у вашій компанії є достатньо запасів, знання - це сила, і більше знань краще.

- Моніторинг

Іншою найбільш очевидною перевагою IoT є моніторинг. Знаючи точну кількість запасів, або якість повітря у вашому домі, можна надати додаткову інформацію, яку раніше не було легко зібрати. Наприклад, знаючи, що у вас мало молока або чорнила принтера, можна врятувати ще одну поїздку до магазину найближчим часом. Крім того, контроль за закінченням терміну дії продукції може і підвищить безпеку.

- Економія часу

За допомогою IoT можна заощадити велику кількість часу. І в сучасному сьогоднішньому житті ми всі можемо використовувати більше часу.

- Економія грошей

Оптимальне використання енергії та ресурсів може бути досягнуто шляхом використання цієї технології та збереження пристроїв під наглядом. Ми можемо бути попереджені у випадку можливих проблемних місць, поломки та пошкодження системи. Таким чином, ми можемо заощадити гроші за допомогою цієї технології.

Найбільшою перевагою IoT є економія коштів. Якщо ціна обладнання для з'єднання та моніторингу буде меншою, ніж сума, заощаджена грошима, то Інтернет речей буде широко прийнятий. IoT принципово виявляється дуже корисним для людей у їхній повсякденній роботі, роблячи комунікацію між приладами більш ефективною, тим самим заощаджуючи та зберігаючи енергію та гроші. Дозволяючи передавати дані та обмінюватися даними між пристроями, а потім переводити їх у потрібний для нас режим.

- Автоматизація

IoT дозволяє автоматизувати та контролювати завдання, які виконуються щодня, уникаючи втручання людини. Зв'язок машина-машина M2M допомагає підтримувати прозорість у процесах. Це також призводить до рівномірності завдань. Цей зв'язок також може підтримувати якість обслуговування QoS. Ми також можемо вжити необхідних заходів у разі виникнення надзвичайних ситуацій.

- Ефективність роботи

Взаємодія між машинами забезпечує кращу ефективність, отже точні результати можна отримати швидко. Це призводить до економії цінного часу. Замість того, щоб повторювати ці самі завдання щодня, це дає можливість людям робити інші творчі роботи.

- Краща якість життя

Всі додатки цієї технології завершуються підвищенням комфорту, зручності та кращого управління, тим самим покращуючи якість життя.

1.6 Недоліки IoT

Тут наведено деякі недоліки IoT:

- Сумісність пристроїв

Оскільки пристрої різних виробників будуть з'єднані між собою, виникає питання сумісності в з'єднанні та моніторингу.[7-8] Хоча цей недолік може знизитися, якщо всі виробники згодні з загальним стандартом, навіть після цього технічні питання будуть зберігатися. Сьогодні у нас є пристрої з підтримкою Bluetooth і проблеми з сумісністю існують навіть у цій технології. Проблеми сумісності можуть призвести до того, що люди купують прилади від певного виробника, що призводить до його монополії на ринку.

- Складність мережі

IoT є різноманітною і складною мережею. Будь-які помилки або

помилки програмного або апаратного забезпечення матимуть серйозні наслідки. Навіть збій живлення може викликати багато незручностей. З Інтернетом речей, помилки можуть зрости до небес.

Наприклад, припустимо, що ви та ваша дружина отримуєте повідомлення про те, що ваше молоко закінчився, і ви обидва зупиняєтеся в магазині на шляху додому, і ви обидва купуєте молоко. Як наслідок, ви і ваша дружина витратили вдвічі більшу суму, ніж вам обом потрібно.

Або, можливо, помилка в програмному забезпеченні автоматично замовляє новий картридж для принтера кожну годину протягом декількох днів, коли вам потрібна лише одна заміна.

- Менша зайнятість людського персоналу

Некваліфіковані працівники та помічники можуть втратити роботу внаслідок автоматизації щоденної діяльності. Це може призвести до проблем безробіття в суспільстві. Ця проблема пов'язана зі створенням будь-якої нової технології та може бути подолана високоякісною освітою. З автоматизованою щоденною діяльністю, природно, буде менше потреб людських ресурсів, насамперед робітників і менш освічених кадрів. Це може створити проблему безробіття в суспільстві.

- Контроль над нашим життям

Наше життя буде все більше контролюватися технологією, і буде залежати від нього. Молоде покоління вже зараз залежне від технології і не може без них обходитись (наприклад, Wi-Fi). Ми повинні вирішити, скільки наших повсякденних функцій ми готові механізувати та зробити керованими технологією.

- Конфіденційність

З усіма даними, що передаються в IoT, ризик втрати конфіденційності збільшується. Наприклад, відбудеться збій роботи та ваші сусіди зможуть побачити ваше фінансове становище, які ліки ви купуєте в магазині та інше.

- Безпека

Оскільки всі побутові прилади, промислове обладнання, послуги державного сектору, такі як водопостачання та транспорт, а також багато інших пристроїв, підключені до Інтернету, багато інформації зберігається в мережі. Ця інформація схильна до атаки хакерів. Було б надзвичайно катастрофічно, якщо до несанкціонованого вторгнення буде доступна приватна та конфіденційна інформація.

1.7 Висновки до розділу 1

В першому розділі було розв'язано такі питання:

- Розглянуто основні терміни мережі Інтернет речей
- Досліджено архітектуру, еталону модель та їх основні компоненти IoT. Наведено характеристики всіх основних елементів
- Розглянуто принципи дії IoT мережі на прикладі найпростішого вигляду архітектури мережі.
- Наведено переваги та недоліки, які притаманні мережам IoT.

Після аналізу переваг та недоліків моделі IoT можна зробити висновок, що попри те, що переваг набагато більше ніж недоліків, на даний момент повноцінне використання Інтернет речей неможливе через проблему безпеки та конфіденційності. Тому поки не будуть повноцінно вирішенні ці дві найважливіші проблеми краще не використовувати Інтернет речей.

2 ОГЛЯД ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОТОКОЛІВ ТА ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ ІОТ

2.1 Технології та протоколи передачі даних на довгі відстані в ІоТ мережах

В найближчому майбутньому до Інтернету речей будуть підключені велика кількість пристроїв. Більша доля цих пристроїв буде мати живлення від батарейок. У зв'язку з цим, однією з основних характеристик є тривалість роботи обладнання без втручання людини.

Для того щоб розв'язати цю проблему були створені нові мережі спеціально для ІоТ. Ці мережі називаються LPWAN (Long Power Wide Area Network). Основними технологіями цих мереж є NB-IoT, Weightless, LoRa, SIGFOX та інші. Ці технології з'явилися через те, що необхідно буде підключати велику кількість датчиків та приладів для централізованого збору інформації на хмарних серверах.[9] Надалі буде наведено основні технології мережі LPWAN.

2.1.1 LoRaWAN

Поява технології LoRaWAN викликало великий резонанс на ринку бездротового зв'язку, що спричинило необхідність прийняти єдиний стандарт для глобальних мереж з низьким енергоспоживанням - LPWAN (Low Power Wide Area Network).[10] Аббревіатура LoRa об'єднує в собі метод модуляції LoRa у бездротових мережах LPWAN, розроблений Semtech та відкритий протокол LoRaWAN.

LoRa (Long Range) - це технологія і однойменний метод модуляції. Метод модуляції LoRa запатентований компанією Semtech, заснований на технології розширення спектру (spread spectrum modulation) і варіацію лінійної частотної модуляції (chirp spread spectrum, CSS), за якої дані закодовано широкосмуговими імпульсами з частотою, що збільшується, або

зменшується на деякому тимчасовому інтервалі.[11] Таке рішення, на відміну від технології прямого розширення спектра, робить приймач стійким до відхилень частоти від номінального значення та спрощує вимоги до тактового генератора, що дозволяє використовувати недорогі кварцові резонатори. LoRa використовує пряму корекцію помилок (forward error correction, FEC), працює в субгігагерцовому діапазоні частот.

LoRa дозволяє демодувати сигнали на рівні 20 дБ нижче рівня шумів, тоді як більшість систем з частотною маніпуляцією (frequency shift keying, FSK) можуть коректно працювати з сигналами на рівні не нижче 8-10 дБ над рівнем шумів. Модуляція LoRa визначає фізичний рівень, який може використовуватися в мережах з різними архітектурами: mesh-мережі, зірка, точка-точка та інші.

Завдяки своїй високій чутливості (148dbm) LoRa ідеально підходить для пристроїв з вимогами низького споживання електроенергії та високої стійкості зв'язку на великих відстанях.

LoRaWAN (Long Range Wide Area Network) — відкритий протокол канального рівня для мереж з високою ємністю та великим радіусом дії і низьким власним використанням енергії, який LoRa Alliance стандартизувала для мереж LPWAN.[10]

Разом з протоколом LoRaWAN можуть працювати декілька видів пристроїв.(див. рис. 2.1)

Ці пристрої в LoRaWAN поділяються на:

- Двонаправлені кінцеві пристрої "класу А" (Bi directional End Devices, Class A). Подібні пристрої застосовуються, коли вимагається підтримувати мінімальну потужність при переважанні передачі даних з сервером. Кінцевий вузол ініціює сеанс зв'язку шляхом відправки пакету даних, після чого виділяє два вікна, в перебігу яких чекає дані від сервера. Відповідно, можливість передачі даних між сервером і кінцевим пристроєм виникає тільки після відкриття сеансу кінцевим пристроєм.

- Двонаправлені кінцеві пристрої "класу Б" (Bi directional End Devices, Class B). Відрізняється від пристроїв "класу А", оскільки має можливість за розкладом відкривати додаткові вікна прийому. Для складання розкладу кінцевий пристрій здійснює синхронізацію за спеціальним сигналом від шлюзу. Таким чином, наявність додаткового вікна надає змогу серверу обмінюватися даними у попередньо обумовлений момент часу.

- Двонаправлені кінцеві пристрої "класу С" з максимальним приймальним вікном (Bi directional End Devices, Class C). Відрізняються практично безперервним вікном прийому даних і закривають його лише на час передачі даних. Така особливість, дозволяє застосовувати їх для вирішення завдань, пов'язаних з великим обсягом даних.



Рисунок 2.1 Типи пристроїв LoRaWAN[10]

Архітектура LoRaWAN складається з таких основних елементів: кінцеві вузли, шлюзи, мережевий сервер, а також сервер додатків.(див. рис. 2.2)

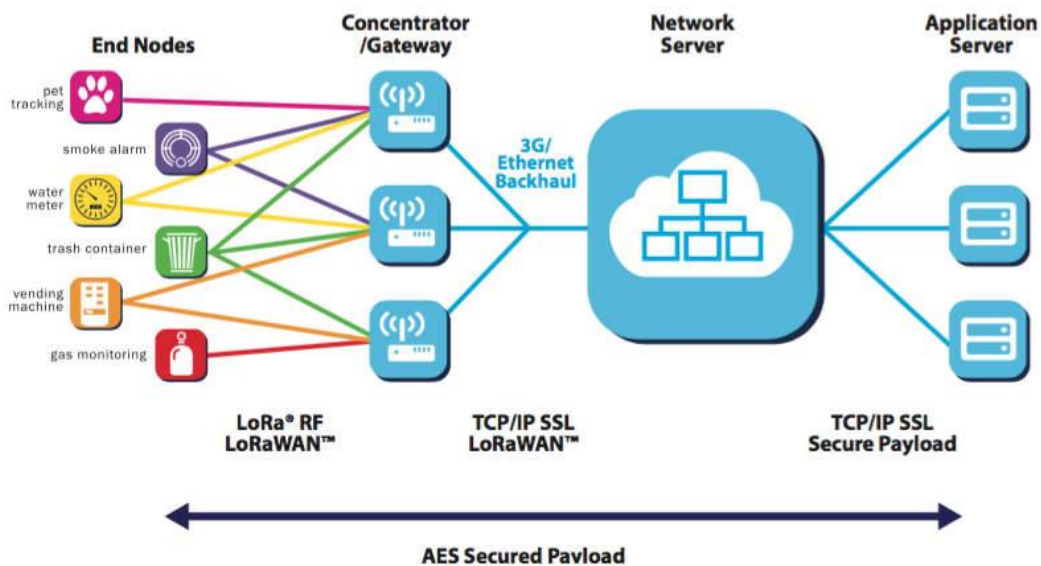


Рисунок 2.2 Архітектура мережі LoRaWAN[10]

Кінцеві вузли (End Nodes) - пристрої, що здійснюють, вимірювання, контроль та управління. Вузол складається з наборів датчиків вимірювання та керуючі елементи. Мають зазвичай живлення від батарейок. Для того щоб економити енергію вузли виконують передачу даних на деякий невеликий проміжок часу, після чого відкривається два тимчасові вікна для прийому даних.

Шлюз LoRa (Gateway/Concentrator) - це пристій, який приймає дані через радіоканал від кінцевих пристроїв та передає їх в транзитну мережу. До транзитних мереж можна віднести WiFi, Ethernet, стільникові мережі і будь-які інші телекомунікаційні канали. Кінцеві пристрої та шлюз утворюють мережеву топологію типу “зірка”. Доволі поширеним є те, що пристій складається з багатоканальних пристроїв прийому та передачі, це дозволяє обробляти сигнали, які одночасно надходять по декількох каналах, або кілька сигналів, отриманих від одного каналу. Таким чином, кілька схожих пристроїв можуть забезпечити повне покриття мережі і прозору двонаправлену передачу даних між мережевим сервером та кінцевими вузлами.

Мережевий сервер (Network Server) — віддалений центр управління мережею. За його допомогою відбувається регулювання швидкості, аналіз, обробка та зберігання даних, що були прийнятими з шлюзу.

Сервер програм (Application Server) - пристрій для збору інформації з кінцевих вузлів та віддаленого контролю їх роботи.

Один LoRa-шлюз допускає обслуговування до п'яти тисяч кінцевих пристроїв, що досягається за рахунок:

- Особливостей топології мережі.
- Адаптивної швидкості передачі даних і адаптивної вихідної потужності пристроїв, що задаються мережевим вузлом.
- Тимчасовим поділом доступу до середовища.
- Частотним поділом каналів.
- Особливістю LoRa модуляції, що дозволяє в одному частотному каналі одночасно демодулювати сигнали, що передаються на різних швидкостях.

Можна сказати, що поява енергоефективних бездротових технологій LoRaWAN дозволило будувати глобальні, і в той же час, більш прості мережі передачі даних з великим числом кінцевих вузлів. Їх відмінні переваги - це розширений радіус дії, довга автономна робота і гарантоване виявлення корисного сигналу на тлі впливу перешкод.

2.1.2 SigFox

SigFox - це технологія, яка приносить нову мережу та інформаційну стратегію IoT. Розробник, група з Labège, Франція з однойменною назвою, SigFox - це мережевий оператор, який займається впровадженням IoT у бізнес індустрію.[12] Архітектура мережі SigFox досить сильно схожа на мережі стільникових операторів зв'язку таких як GSM та GPRS, але являється менш затратною та більш енергоефективною.[9]

Зона, яку покриває SigFox складає близько 30-50 км в міський та сільський місцевості. В містах де дуже багато шумів, діапазон роботи 3-10 км.

На рис. 2.3 представлена архітектура мережі технології SigFox. Загальна топологія мережі була розроблена для забезпечення масштабованої, високопродуктивної мережі, з дуже низькою витратою енергії.

SigFox використовує надвузьку смугу частот UNB (Ultra Narrow Band), на основі радіо технології для підключення пристроїв до глобальної мережі. Використання UNB - ключовий фактор у забезпеченні дуже низького рівня потужності передавача, який буде використовуватися під час стану підтримки надійного з'єднання для передачі даних.

У Європі широко використовується діапазон 868,8 МГц (як визначено в ETSI і CEPT), а у США 915 МГц (як визначено FCC).

Пристрої передають свої повідомлення до базової станції SigFox. За допомогою point-to-point (P2P) протоколу на базову станцію Sigfox підключають до своєї Інтернет бази даних, після отримання і декодування повідомлення, дані надсилаються до її Інтернет бази даних. Нарешті, хмарний сервер SigFox посилає повідомлення на клієнтські сервери та ІТ платформи через інтерфейси прикладного програмування (APIs). (див. рис. 2.3)

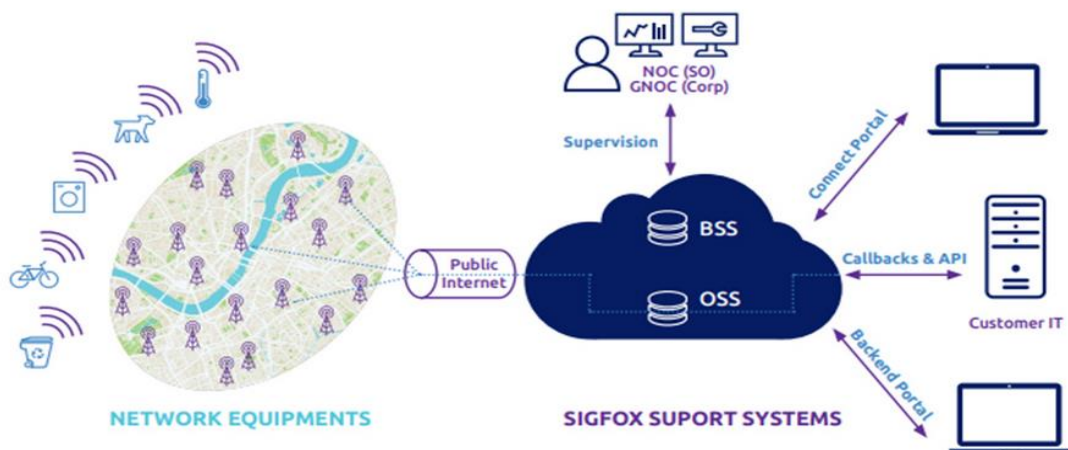


Рисунок 2.3 Архітектура мережі SigFox[13]

Технологія SigFox спрямована на низьку вартість пристроїв, де потребується широка зона покриття.[9] Є цілий ряд додатків, яким необхідна ця технологія бездротового зв'язку. Області, в яких можуть бути використані мережі SigFox включають в себе:

- дім та споживчі товари;
- енергетичні комунікації;
- охорона здоров'я;
- транспорт;
- віддалений моніторинг та контроль;
- безпека.

Стандарт має ряд переваг у порівнянні з іншими базовими технологіями LPWAN мереж. Серед переваг SigFox можна відзначити:

- велика зона покриття;
- висока проникаюча спроможність;
- довга робота від однієї батареї, приблизно до 20 років роботи сенсора від 2-х батарей AA;
- наднизьке енергоспоживання;
- низька вартість.

Як і всі технології сучасного світу, енергоефективна мережу SigFox, на жаль, також має і негативні характеристики:

- низька швидкість передачі даних;
- залежність від стільникової інфраструктури;
- обмежена завадостійкість.

Більшість країн Європи та США використовують саме цю технологію.

2.1.3 NB-IoT

NB-IoT - стандарт стільникового зв'язку створений для приладів телеметрії з низьким об'ємом передачі даних. Створений 3GPP, як розвиток

мобільних стільникових мереж перша версія цього стандарту була представлена в 2016 році. [9]

NB-IoT, або ще його називають стандарт LTE-CAT.M2, має досить велику кількість переваг таких, як низьке енергоспоживання, яке гарантує час роботи батареї до 10 років, широку зону покриття, можливість швидкої модернізації мережі, а також високу надійність.

NB-IoT — це розвиток стільникового зв'язку, який дозволяє операторам працювати з такими напрямками IoT, як системи інтелектуального відслідковування та обліку.

Технологія NB-IoT розглядається як еволюція від стільникового зв'язку до Інтернету речей. Це бездротова різновидність глобальних мереж з низьким споживанням енергії і зроблена для взаємодії між додатками M2M.

Для Nb-IoT можуть використовуватися практично всі ті самі діапазони частот, що і для 2G/3G/4G в "низьких" діапазонах. Це 20 діапазон (800МГц), 8 діапазон (900МГц), 3 діапазон (1800МГц). Більш високі частоти сенсу використовувати немає через більше затухання сигналу.

Є три способи виділення частотного ресурсу для NB-IoT:

- Stand – Alone (автономний).[14]

Виділений частотний канал шириною в 200кГц. Цей варіант найбільш ефективний для роботи NB-IoT, але й найбільш витратний. Справа в тому, що в цьому випадку може знадобитися від 300 до 600 кГц дуже цінного спектру разом із захисними інтервалами. В цьому випадку взаємні інтерференції з іншими технологіями мінімальні (Рис. 2.4).

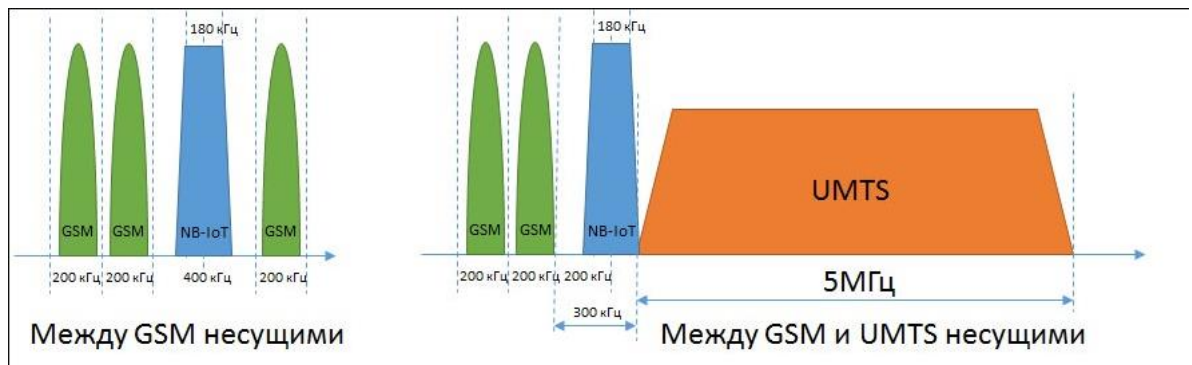


Рисунок 2.4 Варіанти розміщення NB-IoT в режимі Stand - Alone.[14]

- In Band(в середині полоси)

У цьому випадку для NB-IoT виділяються ресурси всередині існуючої LTE несучої, але NB-IoT несуча має підвищену потужність на 6дБ порівняно з ресурсними блоками LTE. Цей варіант добре підходить для економії частотного ресурсу, але при цьому є проблема взаємного впливу з LTE мережею (Рис. 2.5).

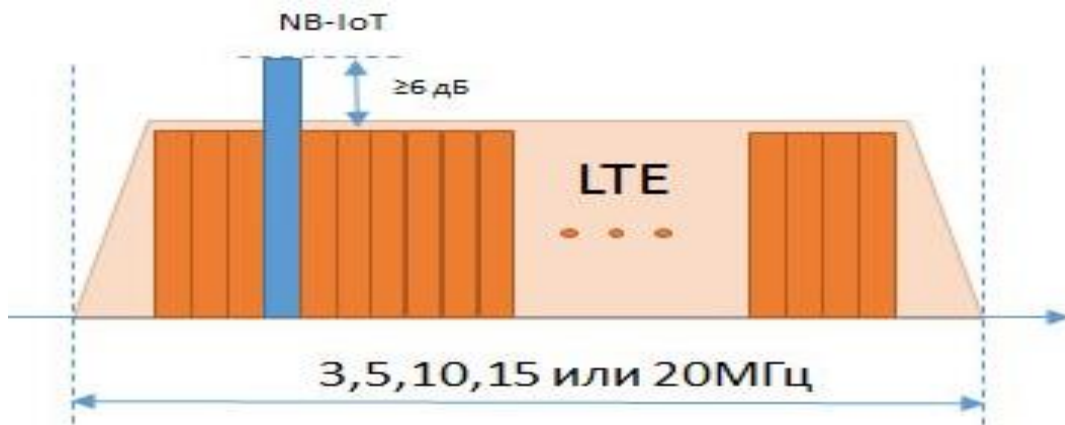


Рисунок 2.5 Розміщення Nb IoT в режимі in Band[14]

- Guard Band(в захистній полосі частот)

В цьому випадку NB-IoT запускається в так званому захисному інтервалі. Наприклад, в смузі LTE 10МГц, по 500 кГц вільного спектру, що використовується в якості захисного інтервалу. Так само як і в режимі in Band для більшої дальності NB-IoT несуча має підвищену потужність на 6-9 дБ порівняно з ресурсними блоками LTE (Рис. 2.6). Цей варіант використання дозволяє одночасно заощадити частотний ресурс і зменшити

взаємний вплив з LTE мережею, хоча в цьому випадку погіршуються параметри позасмугових випромінювань для LTE.

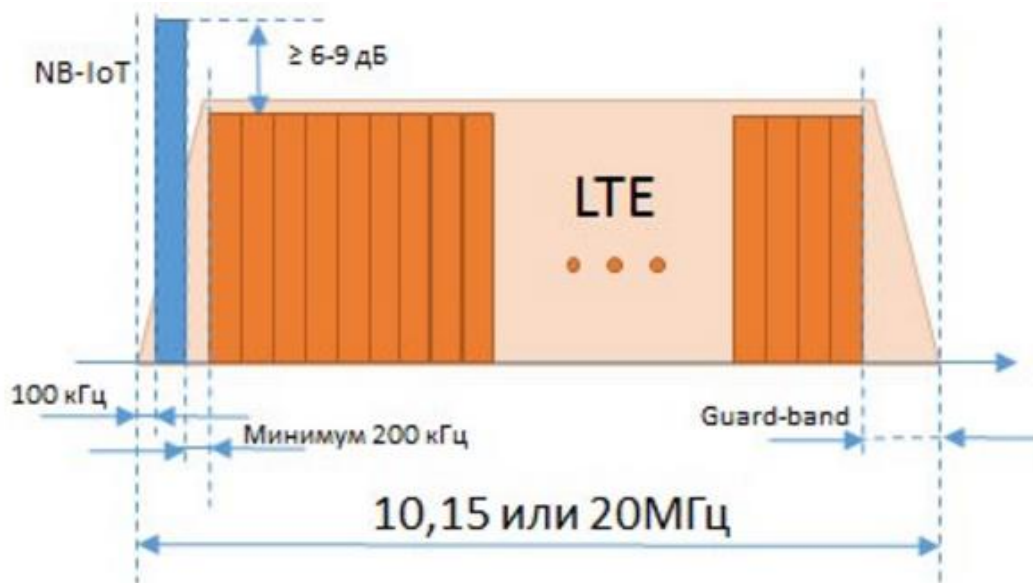


Рисунок 2.6 Розміщення NB-IoT в режимі Guard Band[14]

2.1.4 Weightless-P

Weightless-P — це технологія LPWAN, яка використовується для IoT. Вона використовується в тих випадках, коли потрібна довга служба батареї від одного заряду, двонаправлений зв'язок, а також коли потрібна підтримка високої щільності кінцевих пристроїв.[9] Особливостями цієї технології є широка зона покриття, масштабованість мережі, довгий термін роботи батареї та безпека.

Ця технологія підтримує певний невеликий діапазон груп модуляцій та пропонує можливість двонаправленого зв'язку для забезпечення високої якості зв'язку. Одна базова станція може обслуговувати більшу кількість кінцевих пристроїв, ніж інші технології LPWAN.

Базова станція має контроль над своєю мережею і кінцевими пристроями в будь-який час в інших технологіях базова станція не має таких можливостей.

Weightless-P більш розвинута технологія і вона підтримує гарантовану доставку повідомлень, тому їй не потрібно відправляти повідомлення по декілька разів, як в LoRa, SigFox і через це відбувається економія заряду пристроїв. Також в цій технології використовується метод підтримки адаптивної швидкості передавання інформації і через це забезпечується збільшення терміну служби батареї та підвищується продуктивність роботи мережі.

Також Weightless-P підтримує адаптивну зміну швидкості передачі даних, що забезпечує оптимальну продуктивність мережі і збільшує термін служби батареї кінцевих пристроїв, оскільки він регулює фактичну швидкість передачі даних в залежності від близькості кожного вузла до базової станції. Чим ближче до базової станції кінцеві вузли, тим більш висока швидкість передачі даних, що призводить до більш короткого ефірного часу і більш низької вихідної потужності. Та навпаки вузли, які найбільш віддалені від базової станції, використовують найнижчу швидкість передачі даних і найвищу вихідну потужність.

Більш оптимізований та невеликий по розмірам протокол забезпечує зменшення вартості системи та простоти експлуатації в порівнянні з NB-IoT та іншими стільниковими M2M системами.

Технологія використовується в різних системах спостереження, моніторингу за станом здоров'я людини, розумних речах та ін.

2.1.5 Порівняльна характеристика технологій передачі даних на довгій відстані в мережі IoT

Таблиця 1.1 Порівняння основних технічних характеристик мереж з високою дальністю дії LPWAN

Характеристики	LoRaWAN	SigFox	NB-IoT	Weightless-P
Метод модуляцій	CSS	DBPSK/GFSK	GFSK/BPSK/QPSK	GMSK/PSK
Діапазон	ISM	ISM	Ліцензований	ISM
Швидкість	0,3-50 кбіт/с	100 кбіт/с	UL: 1-144 кбіт/с	0,2-100 кбіт/с (адаптивна)
			DL: 1-200 кбіт/с	
Смуга	Широкосмуг.	Вузькосмуг.	Вузькосмуг.	Вузькосмуг.
	до 500 кГц	100 кГц	200 кГц	12,5 кГц
Максимальний час автономної роботи пристроїв	> 10 років	До 20 років	До 10 років	3-5 років
Частота	868,8 МГц (Європа)	868,8 МГц (Європа)	800/900/1800 МГц	169/433/470/780/868/915 МГц
	915 МГц (США)	915 МГц (США)		
	433 МГц (Азія)			
Безпека	AES-64/128	AES з HMACs	AES-256	AES-128/256
Дальність	До 2,5 км у місті,	До 10 км у місті,	до 2 км	До 2 км у місті
	до 45 км за містом	до 50 км за містом		

2.2 Технології та протоколи передачі даних на короткій відстані в IoT мережах

2.2.1 Z-Wave

Z-Wave — це бездротова радіо технологія з низьким енергоспоживанням. [15] Z-Wave працює в діапазоні частот до 1 ГГц та оптимізована для передавання простих команд для управління з досить малими затримками (зміна гучності телевізора, виключення/включення побутової техніки, зміна яркості екрану тощо).

Вибір частот був зроблений не випадково. Для того, щоб зменшити кількість перешкод від інших технологій, якими вже користуються багато людей, наприклад Wi-Fi сильно навантажений на частоті 2,4 ГГц і тому вже зараз в нашій країні переходять на частоту 5 ГГц.

Технологія Z-Wave - ключ до того, щоб мати повний контроль над вашою домашньою безпекою і енергією, з мінімальними клопотами.[16]

За допомогою технології Z-Wave ви будете мати свою власну домашню систему автоматизації, ви можете програмувати всі основні елементи будинку, такі як освітлення, нагрівання, готування, охолодження і навіть вашу домашню безпеку.

Переваги не закінчуються цим, хоча це - складна система, вона дуже проста у використанні, а також вона ще є енергозберігаючою та економить наш дорогоцінний час.

Система працює за допомогою дистанційного керування і використовує радіохвилі малої потужності. Ця сіткоподібна мережа покриває всі області будинки, оскільки радіохвилі можуть проходити через стіни, поверхи та меблі, роблячи можливість з'єднання надійним майже на 100%.

2.2.2 NFC

Технологія NFC (Near Field Communication) - створена компаніями такими, як Sony та NXP Semiconductors - являє собою комбінування наявних безконтактних технологій зв'язку та радіочастотної ідентифікації.[17]

Технологія NFC призначена для обміну різною інформацією, наприклад, картинками, музичними файлами, номерами телефонів, або ключами цифрової авторизації між двома розташованими близько один до одного пристроями з підтримкою NFC. Це можуть бути смарт-картка, будь-які портативні пристрої, а також зчитувальні пристрої RFID. Дана технологія може використовуватися в якості ключу доступу до даних або служб (електричний замок, або безготівкова оплата).

На відміну від усіх інших технологій безконтактного зв'язку, які можуть передавати дані тільки від активного пристрою до пасивного, NFC може здійснювати обмін інформації між двома активними пристроями.

NFC використовується для взаємодії з пристроями радіочастотної ідентифікації RFID. Для забезпечення сумісності між картами RFID та мобільним телефоном різних виробників виконується перевірка цифрового протоколу і проводиться вимірювання всіх важливих властивостей радіочастотного сигналу: тимчасових характеристик, чутливості та амплітуди приймача в активному режимі, частоти несної амплітуди сигналу.

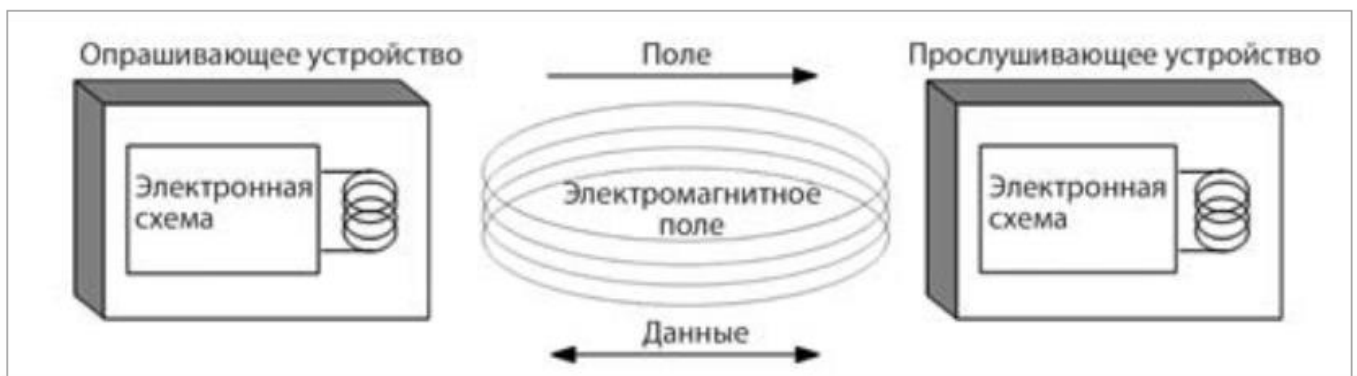


Рисунок 2.7 Принцип роботи NFC[17]

При передачі інформації від активного пристрою до пасивного пристрою використовується амплітудна маніпуляція ASK. При обміні обидва пристрої рівноправні. Кожен пристрій має власне джерело живлення, тому сигнал несної відключається відразу після закінчення передачі.

За рахунок індуктивного зв'язку між опитуваним і прослуховуючим пристроями пасивний пристрій впливає на активне. Зміна імпедансу прослуховуючого пристрою викликає зміну амплітуди або фази напруги на антені опитуваного пристрою. Після цього відбувається з'єднання двох пристроїв та передача даних. Як тільки ми роз'єднуємо два пристрої більш,

ніж на 20 см розривається електромагнітний зв'язок і перестають передаватися дані автоматично.

В дійсності NFC можна вважати, по суті, продовженням вже досить відомої технології радіочастотної ідентифікації RFID.[18] Як ми знаємо, RFID повсюдно використовується в безконтактних картах і мітках. Однак NFC може не тільки зчитувати інформацію з будь-яких пасивних електронних міток, але і здатна забезпечувати двосторонній бездротовий зв'язок між пристроями.

2.2.3 RFID

RFID (Radio Frequency IDentification) - метод автоматичної ідентифікації об'єктів, в якому за допомогою радіосигналів зчитуються або записуються дані, що зберігаються в так званих транспондерах, або RFID - мітках.[19]

Будь-яка RFID - система складається із зчитувального пристрою (зчитувач, рідер) та транспондери (він же RFID - мітка, іноді також називають RFID-тег).

Більшість RFID-міток складається з двох частин. Перша - інтегральна схема для обробки та зберігання інформації, демодулювання та модулювання радіочастотного сигналу і деяких інших функцій. Друга - антена для прийому і передачі сигналу. А також для роботи цих міток потрібне програмне забезпечення — програми, за допомогою яких здійснюється аналіз та збір інформації, одержуваної із RFID-міток.

Мітки бувають двох видів активні та пасивні. Активні мітки мають власне джерело живлення, тому вони можуть самі посилати сигнал і зчитуватися з досить великої відстані. Пасивні мітки не мають власного джерела енергії і активізуються, тільки після того, коли надходить сигнал до пристрою зчитування і тоді передають записану в них інформацію.

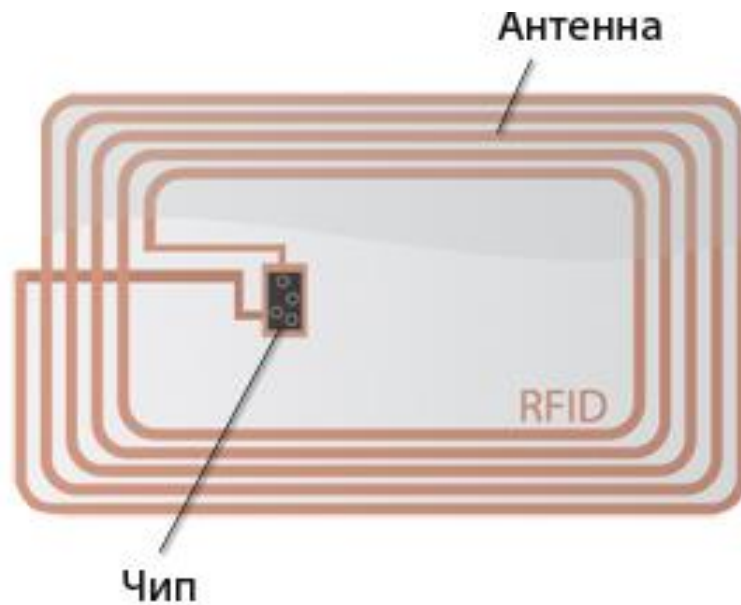


Рисунок 2.8 Будова RFID-мітки[38]

RFID-мітки можуть використовуватися для управління товарними запасами або відстеження часу на спортивних змаганнях.[20] Магнітні мітки не замінюють штрих-коди, а їх доповнюють можливістю дистанційного зчитування. Мітками можуть маркувати велику рогату худобу для запису інформації про проходження ветеринарного огляду. Рішення для транспорту допомагають ідентифікувати автомобіль, навіть якщо вона рухається на великій швидкості. Деякі авіалінії користуються мітками для ефективного відстеження великих потоків багажу. Також RFID вбудовується у біометричні паспорти, кредитні картки для безпечного доступу в захищені області.

Деякі мітки можуть бути прочитані на відстані декількох метрів від прямої видимості пристрою зчитування. Більшість міток представляють собою звичайний текстовий запис та штрих-код в якості доповнення для прямого зчитування у випадках несправності радіочастотної електроніки.

2.2.4 Bluetooth Low Energy

Бездротова технологія з низьким енергоспоживанням Bluetooth (BLE) – це частина специфікації Bluetooth, яка починається з покоління Bluetooth 4.0 і на даний момент закінчується Bluetooth 5.0.[21]

Пристрої, що використовують BLE, споживають менше енергії, ніж інші версії Bluetooth - пристрої попередніх поколінь. У багатьох випадках пристрої зможуть працювати більше року на одній невеличкій батарейці типу таблетка без підзарядки. Завдяки цьому, можна буде використовувати датчики невеликих розмірів, які будуть постійно працювати та взаємодіяти з іншими пристроями.

Основними рівнями BLE є:

- Додаток – реалізує корисну для кінцевого користувача логіку роботи.[22]
- Основний пристрій, або хост – надає верхні рівні стеку протоколів Bluetooth.
- Контролер – займається нижніми рівнями стеку протоколів Bluetooth.

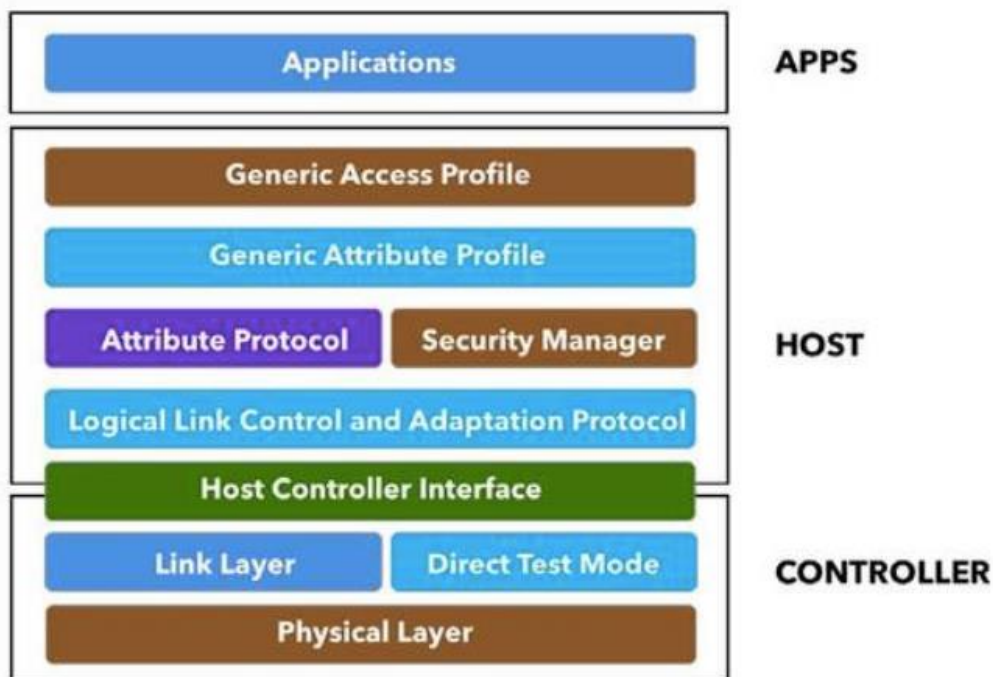


Рисунок 2.9 Архітектура BLE[22]

Рівень додатків – найвищий рівень стеку протоколів.

Рівень хосту містить такі підрівні:

- GAP (Generic Access Profile) – профіль загального доступу;
- GATT (Generic Attribute Profile) – профіль загальних атрибутів;
- ATT (Attribute Protocol) – протокол атрибутів;
- SM (Security Manager) – менеджер безпеки;
- L2CAP (Logical Link Control and Adaptation Protocol) – протокол

логічного з'єднання та адаптації;

- HCI (Host Controller Interface) – інтерфейс хост-контролеру, на стороні хосту.

Рівень контролеру зв'язан за допомогою протоколу HCI та має такі рівні:

- HCI (Host Controller Interface) – інтерфейс хост-контролеру, на стороні контролеру;
- LL (Link Layer) – канальний рівень;
- PHY – фізичний рівень.

BLE призначений для тих пристроїв, які мають невеликі розміри, тобто для пристроїв, у яких важлива компактність і куди не можна встановити повноцінний акумулятор, або батарею великого об'єму.[23] Bluetooth LE споживає в 10-20 разів менше енергії і цілком здатний передавати дані в 50 і більше разів швидше та на відстані більше 100 метрів, ніж класичні Bluetooth рішення.

Крім перерахованих вище переваг, BLE має високу безпечність, надійність, низьку затримку при підключенні та низьку споживчу потужність. Є ще одна важлива особливість даного стандарту, вона полягає в адаптивності переналаштування частоти, тобто відбувається захист від помилок при передачі сигналу, BLE швидко змінює свою робочу частоту, вибираючи найбільш оптимальну для усунення перешкод, проблем переповнення і для зниження інтерференції.

Специфікація Bluetooth 5.0 була створена, з орієнтацією на Інтернет речей. Це остаточно показало, що стандарт прагне "захопити" ринок пристроїв.

В порівнянні з попередньою версією 4.0 була підвищена швидкість передачі даних майже до швидкостей HSPA і LTE ранніх версій, при цьому енергоспоживання залишилося в колишніх показниках. Важливим показником для побудови мереж Інтернету речей як раз є енергоефективність. В даний момент дана специфікація є мало поширеною через те що вона з'явилася нещодавно. Bluetooth 5 як і всі попередні версії має зворотну сумісність. Цілком можливо, через декілька років кожний мобільний пристрій буде підтримувати 5 версію цього стандарту, що є найважливішою перевагою цієї технології над іншими.

2.2.5 Wi-Fi HaLow

Wi-Fi HaLow — це протокол бездротової мережі, опублікований у 2017 році, як доповнення до стандарту бездротової мережі IEEE_802.11.[24] Цей протокол працює на непотребуючій ліцензування частоті 900 МГц, для забезпечення розширеного діапазону Wi-Fi мереж, порівняно зі звичайними мережами Wi-Fi, працюючими в діапазонах 2,4 ГГц і 5 ГГц. Його низьке енергоспоживання також є перевагою, таким, що дозволяє створювати великі групи станцій або датчиків, які взаємодіють щоб поширювати сигнали, підтримуючи концепцію інтернет-речей (Internet of Things, IoT). Низьке енергоспоживання протоколу конкурує з Bluetooth і має додаткову перевагу - вищі швидкості передачі даних і більш широкий діапазон покриття.(див. рис. 2.10)

Wi-Fi HaLow дозволить розширити можливості енергоефективного сценарію використання розумного будинку, автомобілів, а також в торгівлі, промисловості, сільському господарстві тощо.

Wi-Fi HaLow розширює Wi-Fi в діапазоні 900 МГц, даючи можливість з'єднання пристроїв малої потужності, таких як датчики та портативні комп'ютери. Wi-Fi HaLow успадкує позитивні якості попередніх протоколів, такі як надійний захист інформації, широку сумісність обладнання та простоту встановки.

Пристрої з підтримкою Wi-Fi HaLow будуть також працювати у діапазонах 2,4 та 5 ГГц, що дасть можливість інтегрування в екосистему, яка на даний момент налічує більше 7 млрд пристроїв. Також Wi-Fi HaLow буде мати підтримку підключення по IP, це дозволить працювати з хмарами, що дуже важливо для IoT. Також буде можливість підключатися до одієї точки доступу близько 1000 пристроїв.

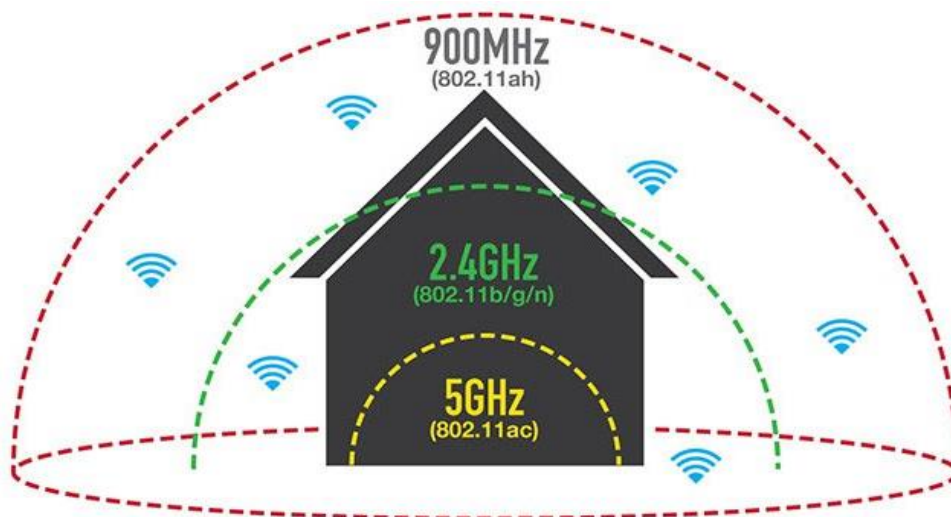


Рисунок 2.10 Порівняння різних протоколів Wi-Fi за зоною покриття

2.2.6 Порівняльна характеристика технологій та протоколів передачі даних на короткі відстані в IoT

Таблиця 1.2 Порівняння основних технічних характеристик мереж з низькою дальністю дії

Характеристики	RFID	NFC	BLE	Z-Wave	Wi-Fi HaLow
Смуга частот	6/13.5/433/863-870/902-928 МГц	13.56 МГц	2.4 ГГц	868/915 МГц	Піддіапазон 1 ГГц
	2.4/5-27 ГГц				
Швидкість передачі даних	500 кбіт/с	106/212/424/848 кбіт/с	1 Мбіт/с	9.6,40 та 100 кбіт/с	До 4 Мбіт/с
Радіус дії	0.1 - 5 м	0.1 м	70 м	100 м	100 – 1000 м
Пропускна здатність на канал	10 МГц для 6 МГц	Змінна	40 каналів з шириною в 2 МГц	300,400 кГц	1/2/4/8/16 МГц
	14 МГц для 13.5 МГц				
	1.74 МГц для 433 МГц				
	7 МГц для 800 МГц				
	8 МГц для 2.4 ГГц				
	5 – 27 ГГц сегментований				
Модуляція	-	ASK, BPSK	GFSK	FSK/GFSK	BPSK, QPSK, 16-/64-/256-QAM, OFDM
Топологія	Point to Point	Peer-to-peer	Single-hop	Mesh	Star
	Point to Multipoint				
Безпека	Шифрування	Шифрування	AES-128	AES-128	WPA

2.3 Протоколи для передачі повідомлень

2.3.1 Проблематика передачі повідомлень в мережі IoT

Обсяг інформації, що формується одним сенсорним вузлом, порівняно невеликий, однак більшість сервісів Інтернету речей побудовано на принципі обробки інформації від безлічі вузлів, що принципово відрізняється від

архітектур, прийнятих в класичних мережах, типу абонент - вузол зв'язку для телефонії, клієнт - сервер для передачі даних. [25]

Таким чином, ми стикаємося з новою архітектурою: багато джерел - багато одержувачів, крім того, обсяг трафіку від сенсорного вузла може бути як дуже маленьким, так і дуже великим. Звичні прикладні протоколи для передачі повідомлень не розраховані на таке використання.

2.3.2 Базова топологія, яка використовується для передачі повідомлень в IoT

Представлена топологія на рис. 2.11 відповідає шаблоном проектування передачі повідомлень, який має назву "видавець-підписник" (Publisher-Subscriber, або pub/sub). У такій схемі вводиться поняття видавця – джерела інформації та передплатника – одержувача інформації. Термін підписка пов'язаний з певною операцією, виконаною учасниками, з метою отримання інформації передплатником від конкретного видавця, а також упорядкування збору інформації – параметрів періодичності отримання та аналогічних (в залежності від реалізації) показників.

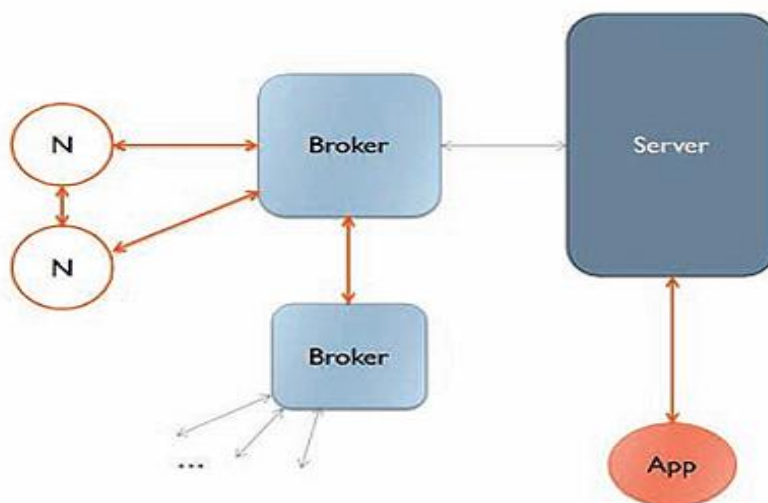


Рисунок 2.11 Топологія системи, яка виконує передачу даних між різними вузлами мережі IoT[25]

В даному випадку розглядається ситуація, коли сенсорний вузол (Node) об'єднує інформацію від багатьох датчиків (наприклад, дані вологості повітря) і направляє її згідно з параметрами передплати або за запитом, або самостійно через певний інтервал часу. Зазвичай самі датчики досить примітивні, їх завдання зводяться до постійної передачі інформації про контрольовані параметри. Тому з'являється необхідність об'єднувати датчики в вузли, оснащені мікроконтролерами, які будуть відповідати за зчитування вимірюваних даних і відправку їх за заздалегідь визначеними алгоритмами далі на сервер. Також найчастіше для взаємодії клієнта з системою необхідна ще клієнтська програма (Application), встановлена на персональному пристрої, яка необхідна для наочного представлення одержуваної від датчиків, або вже обробленої сервером інформації та управління системою. Така топологія також розрахована на включення брокера (Broker). Брокер – це сервер, який приймає інформацію від видавців і передає її відповідним передплатникам, в складних системах може виконувати, також різні операції, пов'язані з аналізом та обробкою даних, що надійшли на сервер. Брокер може встановлювати пріоритети сполученням і формувати черги для передачі повідомлень. Таким чином брокер організовує пересилання повідомлень, їх зберігання та фільтрацію. Під чергою повідомлень розуміється контейнер, або блок, в якому зберігаються повідомлення в процесі їх пересилання. При недостатньому ресурсі каналу зв'язку, або якщо одержувач недоступний під час того, як надсилається повідомлення, черга зберігає повідомлення до тих пір, поки воно не буде доправлено до відправника.

2.3.3 DDS

DDS (Data Distribution Service) - протокол прикладного рівня M2M для систем реального часу. Базується на моделі "видавець-передплатник". Основна функція протоколу полягає в тому, щоб здійснити з'єднання пристроїв з іншими пристроями за допомогою шини обміну повідомленнями

(див. рис. 2.12). Протокол DDS може ефективно та синхронно доставляти мільйони повідомлень в секунду.

Пристрої дають запит на дані інакше, ніж в ІТ мережах.[27] По-перше, пристрої працюють швидко. Масштаб реального часу часто вимірюється в долях мікросекунд. Пристроєм потрібно здійснювати зв'язок з іншими пристроями, використовуючи складні шляхи, тому прості і надійні двоточкові TCP потоки даних обмежують можливості для такої передачі. Натомість DDS забезпечує деталізований контроль якості обслуговування (QoS), багатоадресну передачу, переналаштовану надійність і всеосяжну надмірність. Крім того, сильною стороною DDS є розгалуження даних. Протокол DDS забезпечує потужні способи фільтрації та відбору даних за адресами призначення, причому число синхронних одержувачів даних може обчислюватися тисячами. Деякі пристрої досить компактні, тому існують полегшені версії протоколу DDS, які працюють в умовах обмеженого обсягу.

Для використання даних від пристроїв зіркоподібна мережа зовсім не годиться. Замість цього DDS реалізує пряму шинний зв'язок між пристроями на базі реляційної моделі даних. Її називають шиною даних (DataBus), оскільки це мережевий аналог бази даних (database).(див.рис.)

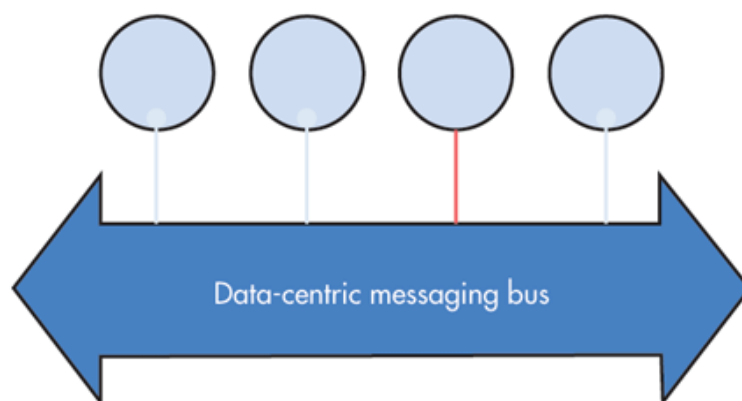


Рисунок 2.12 Принцип з'єднання пристроїв за допомогою протоколу DDS в IoT[26]

Подібно до того, як база даних управляє доступом до збережених даних, шина даних управляє доступом до даних та оновленнями одночасно

багатьох користувачів. Це саме те, що потрібно високопродуктивним пристроям, щоб вони працювали разом, як єдина система.

Високопродуктивні системи інтегрованих пристроїв використовують протокол DDS. Це єдина технологія, яка забезпечує гнучкість, надійність та швидкість, необхідні для побудови складних додатків реального часу. Ці додатки містять в собі військові системи, вітроелектростанції, інтегровані системи лікарень, системи діагностичної візуалізації, системи супроводження ресурсів і автомобільні системи випробувань і забезпечення безпеки.

2.3.4 XMPP

XMPP (eXtensible Messaging and Presence Protocol) - відкритий, заснований на XML, вільний для використання протокол для миттєвого обміну повідомленнями та інформацією про присутність в режимі, близькому до режиму реального часу.[28] Спочатку спроектований легко розширюваним, протокол, крім передачі текстових повідомлень, підтримує передачу голосу, відео та файлів через мережу.

В протоколі XMPP використовується текстовий формат XML в якості вбудованого типу, забезпечуючи природний зв'язок між людьми. Протокол працює по TCP, або за допомогою HTTP поверх TCP. Його перевагою є метод адресування за допомогою ідентифікаторів Jabber ID, який містить в собі наступні, такі компоненти як вузол, домен та ресурс, причому два останні компоненти не є обов'язковими. Адрес має такий вид username@gmail.com, який допомагає з'єднувати користувачів у величезному просторі Інтернету. XMPP підтримує різні комунікаційні моделі (запит-відповідь, публікація, підписка та інші).[25]

XMPP забезпечує простий спосіб адресуванні пристроїв. Це особливо зручно, коли дані передаються між віддаленими, найчастіше незалежними точками, як у випадку зв'язку між двома абонентами. Цей протокол не володіє високою швидкістю. Фактично, в більшості реалізацій цього

протоколу використовується метод опитування або перевірки доповнень тільки на вимогу.

Сильними сторонами цього протоколу також є безпека, масштабованість, тому він ідеально підходить для невеликих мереж Інтернету речей.

2.3.5 CoAP

CoAP (Constrained Application Protocol) - це спеціалізований протокол передачі, розроблений робочою групою IETF-CORE, створений для мереж і пристроїв з обмеженими ресурсами, M2M додатків.[25] CoAP можна розглядати як доповнення до HTTP, але на відміну від HTTP CoAP націлений на використання в пристроях з певними обмеженнями. CoAP використовує транспортний протокол UDP.

Повідомлень, використовуваних протоколом CoAP, не так багато, більшість з них це запити відповіді: GET(отримати інформацію з приводу ресурсу), PUT(задати нове завдання над ресурсом), POST(зміна дій над ресурсом), DELETE(видалити активні можливості ресурсу), CONNECT(з'єднання). Клієнти (додатка користувача) використовують повідомлення для управління і спостереження за ресурсом. За запитом встановлюється прапор спостереження, і сервер продовжує відповідати після того, як початкове повідомлення було передано. Це дозволяє серверам організовувати потокову передачу змін станів датчиків.

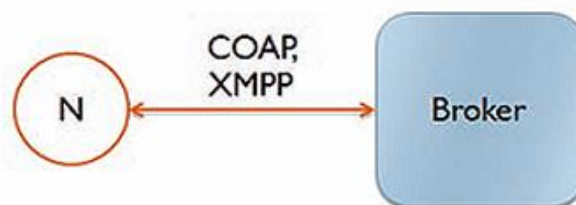


Рисунок 2.13 Сегмент мережі де використовується протокол CoAP та XMPP

Таким чином, на ділянці мережі між сенсорним вузлом і брокером для забезпечення їх зв'язку, з метою реєстрації та конфігурації вузлів, а також для передачі інформації найчастіше застосовуються два протоколи - XMPP та CoAP. Фактичний протокол протоколу залежить від умов, які реалізується на мережі. Можна відзначити, що XMPP знайшов своє застосування в системах освітлення і клімату, а також використовується для адресування пристроїв в невеликих персональних мережах. Очевидно, що CoAP призначений для пристроїв з обмеженими ресурсами й для мереж з низьким енергоспоживанням. Відомо застосування протоколу в системах датчиків температури та інших датчиків розумного будинку.

2.3.6 MQTT

MQTT (Message Queue Telemetry Transport) - це легкий, компактний і відкритий протокол обміну даними створений для передачі даних на віддалених локаціях, де потрібний невеликий розмір коду і є обмеження до пропускної здатності каналу.[29] Перераховані вище вимоги дозволяють застосовувати його в системах M2M (машина-машина).

Також існує версія протоколу MQTT-SN (MQTT для мереж датчиків), раніше відома як MQTT-S, яка призначена для вбудованих бездротових пристроїв без підтримки TCP/IP мереж.

На рисунку 2.14 представлений загальний формат повідомлень протоколу MQTT. Повідомлення складається з двох заголовків:

- MQTT Fixed Header – заголовок фіксованої довжини;
- Variable Length Header – заголовок змінної довжини (в залежності від типу повідомлення);
- Variable Length Message Payload – поля корисного навантаження змінної довжини.

До заголовка фіксованої довжини входять такі поля:

- Message Type – тип повідомлення,
- DUP – прапор дублювання повідомлення,
- QoS Level – рівень якості обслуговування,
- Retain – спеціальний прапор збереження останнього прийнятого брокером повідомлення,
- Remaining Length – залишкова довжина,

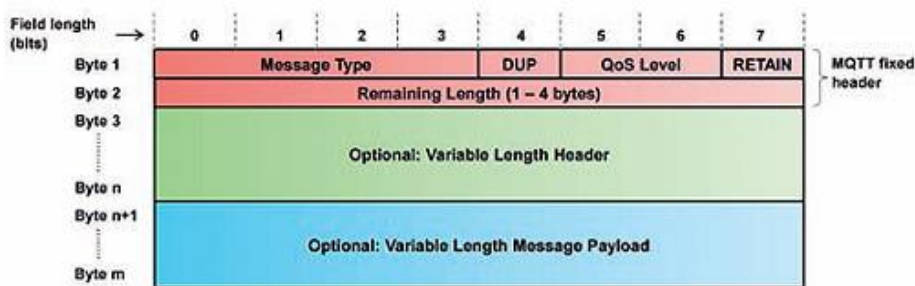


Рисунок 2.14 Загальний формат повідомлення протоколу MQTT[29]

Спрощений процес роботи протоколу MQTT:

Видавець передає повідомлення з певними даними (наприклад, інформація з датчиків вологості) на брокера, вказуючи при цьому тему (Topic), до якої ці дані відносяться (наприклад, "вологість").(див. рис. 2.15) [30]

Брокер аналізує, які із передплатників мають підписку на певні теми, в даному випадку – на тему "вологість".

Передплатникам, які підписані на тему "вологість", брокером буде відправлено повідомлення з інформацією від датчиків вологості.

Таким чином, безліч передплатників можуть бути підписані на різноманітні теми і в залежності від цих підписок отримувати необхідну їм інформацію, не спілкуючись з видавцем безпосередньо. На рис. 2.15 зображено схему передачі інформації за принципом "видавець-передплатник".

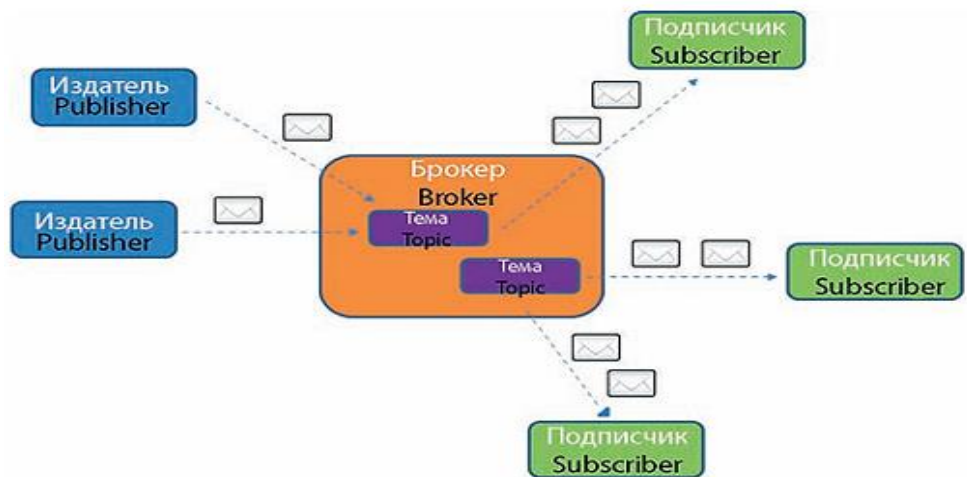


Рисунок 2.15 Принцип роботи протоколу MQTT[30]

2.3.7 STOMP

STOMP - Simple (або Streaming) Text Oriented Message Protocol - простий протокол обміну повідомленнями, що передбачає широку взаємодію з багатьма мовами, платформами та брокерами [25]. Даний протокол підходить під шаблон "видавець-передплатник" і за допомогою повідомлень SEND (відправити), SUBSCRIBE (підписатися), UNSUBSCRIBE (відписатися), BEGIN (почати), ABORT (переривати), ACK (підтвердити), NACK(не підтвердити), DISCONNECT(відключити) організовує зв'язок з брокером за методом "запит-відповідь".

Цей протокол використовується в тих випадках, коли необхідно застосування простого протоколу передачі повідомлень в мережах, що мають обладнання різних платформ.

Протокол схожий на HTTP, використовує транспорт TCP, є простим текстовим протоколом, що дозволяє клієнтам STOMP спілкуватися з будь-яким брокером повідомлень, котрі підтримують цей протокол. Таким чином, цей спосіб взаємодії, розроблений для обміну повідомленнями між платформою, описаною одною мовою програмування, і клієнтом, програмне

забезпечення якого розроблене іншою мовою. Підтримує велику кількість сумісних клієнтських бібліотек.

Треба відзначити, що для забезпечення роботи брокера в мережі Інтернету речей можливе використання обох протоколів: MQTT і STOMP.(див. рис. 2.16) Тільки протокол STOMP орієнтований тільки на взаємодію брокера з сервером, а протокол MQTT забезпечує "наскрізний" зв'язок, як від брокера до сенсорних вузлів, так і від брокера до сервера.

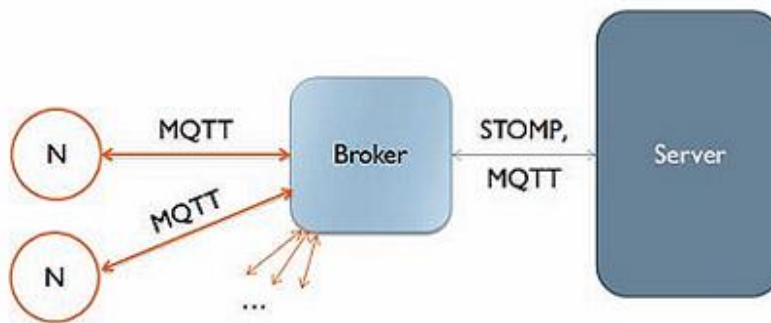


Рисунок 2.16 Сегмент мережі де використовується протокол MQTT та STOMP[25]

2.3.8 SOAP

SOAP (Simple Object Access Protocol) - протокол обміну структурованими та довільними повідомленнями формату XML в розподіленому обчислювальному середовищі.[25] SOAP використовує базову модель з'єднання, що забезпечує узгоджену передачу повідомлення від відправника до одержувача, потенційно допускає наявність посередників, які можуть обробляти частину повідомлення або додати до нього додаткові елементи.

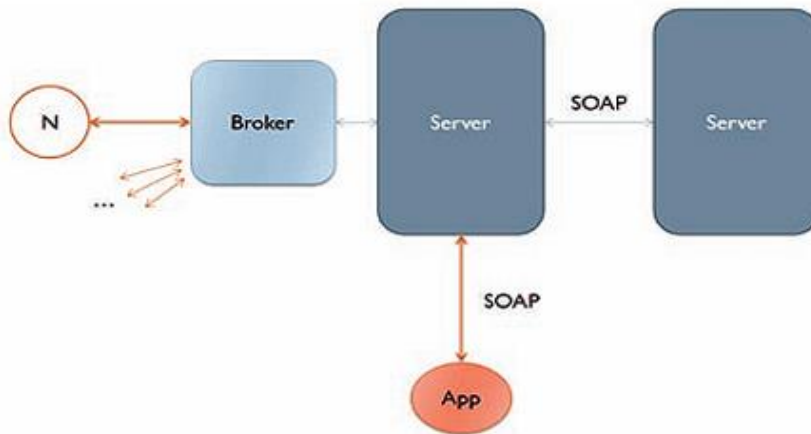


Рисунок 2.17 Сегмент мережі де використовується протокол SOAP[25]

SOAP підтримує два механізми доступу - SOAP MESSAGE та SOAP RPC.[31]

SOAP MESSAGE - це протокол для відправлення та обробка SOAP повідомлень, заснований на об'єкті Message. Може використовуватися для асинхронних комунікацій та має на увазі негайну, або відкладену відповідь на запит.

SOAP RPC являє собою простий протокол "запит-відповідь", який базується на об'єкті Call. Цей об'єкт використовується для синхронного віддаленого виклику процедур за допомогою XML.

Завдяки декільком повідомленням (GET, SOAP ACTION-RESPONSE, SOAP ACTION), який передбачає запит-відповідь, протокол може використовуватися з будь-яким протоколом прикладного рівня: FTP, HTTPS, SMTP.

2.3.9 Порівняльна характеристика протоків передачі повідомлень

Таблиця 1.3 Порівняння розглянутих протоколів

Протокол	Транс.	Призначення	Особливості
DDS	UDP	Для мереж, що потребують розподіленого навантаження	Реалізує прямий шинний зв'язок між пристроями на базі реляційної моделі даних
XMPP	TCP	Для адресації в невеликій персональній мережі	Для ідентифікації користувачів використовуються JID, по формату схожі на адреса електронної пошти (username@gmail.com)
COAP	UDP	Для мереж з обмеженими ресурсами, низьким електроспоживанням	Враховує різні питання середовища реалізації в обмежених мережах
MQTT	TCP	Для завантажених мереж з великою кількістю пристроїв та брокером	Використання механізму черг повідомлень
STOMP	TCP	Для мереж, в яких є можливість використання декількох комбінацій різних протоколів, що потребують простий протокол передачі повідомлень через брокера	Взаємодія з більшістю мов, платформ та брокерами
SOAP	TCP	Для розподіленої обчислювальної мережі	Підтримує два механізми доступу: SOAP RPC та SOAP Message

Таблиця 1.4 Операції, що виконуються аналізованими протоколами

Протокол	Операції	Відмінні особливості
DDS	Процедури отримання та відправки даних	Реалізує прямий шинний зв'язок. “Зберігання історії” – наявність кешу. Підтримка механізму контролю “життєдіяльності” (Keep-alive та Lifecycle)
XMPP	Процедури запиту інформації/вимог, отримання даних, встановлення нових значень, або заміщення існуючої величини	XML-потоків та XML-строфи забезпечують швидкий асинхронний обмін. Схема адресації JID – набір елементів, що утворюють доменний ідентифікатор, ідентифікатор вузла та ресурсу
COAP	Процедури запису та отримання необхідних конкретних параметрів	Представляє собою двійкову версію протоколу HTTP, спрощену під задачі транспортування даних по лініям з обмеженою пропускну здатністю
MQTT	Процедури обробки публікацій/підписки	Підтримує різні класи якості обслуговування QoS (1-3). Підтримує механізми черг

Продовження таблиці 1.4 Операції, що виконуються аналізованими
протоколами

STOMP	Процедури публікацій/підписки. Операції з транзакціями	Підтримує операції з транзакціями. Підтримка великої кількості спільних бібліотек.
SOAP	Віддалений виклик методів. Процедури запитів параметрів	Можливість віддаленого виклику методів/функцій за допомогою механізму доступу SOAP RPC. Нейтральний до платформи

2.4 Висновки до розділу 2

В другому розділі було розв'язано такі питання:

- Розглянуто основні технології та протоколи передачі даних на довгі дистанції, які входять до складу мереж LPWAN: LoRaWAN, SigFox, NB-IoT, Weightless-P. Здійснена порівняльна характеристика протоколів та технологій передачі даних на довгі відстані таких, як метод модуляції, діапазон частот, швидкість передачі даних, смуга частот, швидкість передачі даних, максимальний час автономної роботи пристроїв, частоти на яких працюють дані технології, рівень безпеки, дальність переді даних.
- Розглянуто основні технології та протоколи передачі даних на короткі відстані, які входять до складу мереж WPAN та WLAN: Z-Wave, RFID, Bluetooth Low Energy та Wi-Fi HaLow. Здійснена порівняльна характеристика протоколів та технологій передачі даних на короткі відстані таких, як смуга частот, швидкість передачі даних, радіус дії, пропускна здатність на канал, вид модуляції, топологія, безпека, довжина пакету.
- Розглянуто проблематику, топологію та здійснений огляд основних протоколів передачі повідомлень в IoT. Здійснена порівняльна характеристика за такими показниками: протокол транспортного рівня, який використовується для передачі повідомлення до користувача IoT, призначення та особливості протоколу, а також операції, які він виконує в мережі IoT.

3 СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ ІОТ В УКРАЇНІ

3.1 Сучасний стан технологій передачі даних в Україні

Найбільші телекомунікаційні компанії України вже почали впроваджувати технології передачі даних в IoT. На даний момент існують дві найпоширеніші технології для передачі даних на великі відстані, які є актуальними на території України серед них: LoRaWAN та NB-IoT.

Основною різницею першої технології передачі від другої в тому, що LoRaWAN працює в неліцензованій частині спектру, а мережа NB-IoT працює в ліцензійній частині спектру на частотах, де використовуються мережі 4G. Перевагою для операторів зв'язку вибрати мережі NB-IoT є те, що можна використовувати вже дійсну архітектуру мережі.

На даний момент компанія Lifecell вирішила йти по більш складному напрямку розвитку мережі IoT та вирішила будувати нову мережу, що використовує технологію LoRaWAN. Компанія Lifecell аргументувала свій вибір тим, що протокол LoRa, на якому працює технологія LoRaWAN працює на більш низьких частотах та забезпечують покриття більшої території, ніж NB-IoT, який працює на частотах 1800 МГц. Оператор вирішив використовувати для цього частоту в 868 МГц. Така технологія дозволить підтримувати зв'язок між пристроями на відстані до 15 км при мінімальному використанню енергії.

На даний момент Lifecell разом з IoT Ukraine встановили більше 80 базових станцій. Вже три обласні центри України получили доступ до Інтернету речей в Києві, Львові та Кропивницькому. Цих базових станцій достатньо для покриття 90% відсотків територій цих міст і вже здійснили підключення перших клієнтів.

Під час реалізації цього проекту тестувалися онлайн-рішення для “розумного” міста, моніторингу навколишнього середовища, логістичних сервісів, “розумного” будинку та ін.

Найбільшого попиту серед компаній користувались наступні послуги:

облік витрат на водопостачання, газу та електроенергії, розумне освітлення, стеження, моніторинг відкриття дверей, а також моніторинг вологості та температури в приміщеннях. На даний момент послугами технологій Інтернету речей користуються більше, ніж 10 бізнес-компаній різних галузей.

Vodafone Україна в лютому 2019 року повідомив про завершення тестування технології NB-IoT в найбільших містах України. NB-IoT пристрої можуть обмінюватися між собою даними на частоті 1800 МГц. При цьому ця технологія дозволяє отримувати стабільний доступ до мережі навіть у важкодоступних місцях, таких як шахти ліфту та підвали.

Оскільки розгортання технології NB-IoT відбулося на базі мережі LTE, то користувачі та партнери отримують високий стандарт безпеки – шифрування та автентифікацію на базі sim-карти, що недоступно для таких технологій, як LoRa. Також технологія NB-IoT дозволяє оптимізувати енергозбереження, збільшуючи термін життя батареї пристроїв до 10 років. При цьому, ємність мережі значно вища, ніж в голосовій мережі, при необхідності є можливість легко виконати масштабування.

3.2 Перспективи розвитку технологій передачі даних в Україні

На даний момент найбільш очікуваною та перспективною технологією, яка дасть більший поштовх до розвитку IoT в Україні та у світі є технологія 5G. Експерти вважають, що мережа 5G у світі буде повноцінно розгорнута лише в кінці 2020 року, а масштабне впровадження відбудеться тільки в 2025 році. Оскільки в Україні тільки в минулому році почалося впровадження мережі 4G чекати найближчі декілька років на мережу 5G не має сенсу.[35]

Підтримка набагато більшого діапазону частот є головною перевагою 5G, наслідком чого є збільшення швидкості передачі даних. 5G швидше, ніж 4G в десятки разів. На даний момент максимальна швидкість передачі даних в 4G становить 100Мб/с, в цей показник складає 10 Гбіт/с.[36]

Ще одною особливістю 5G є нульова затримка та безперебійність. Затримка зменшилася також у 10 разів у мережі 4G вона становила 10 мілісекунд, в 5G до 1 мілісекунди. Це дозволяє передавати дані практично в реальному часі.

Покоління	1G	2/2,5G	3G	4G	5G
Початок розробок/реалізація	1970/1984	1980/1999	1990/2002	2000/2010	2015/2020
Швидкість передавання	2 кбіт/с	14,4-64 кбіт/с	2 мбіт/с	100 мбіт/с	1 гбіт/с
Стандарти	AMPS TACS NMT	TDMA CDMA GSM PDC	WCDMA CDMA2000 UMTS	Єдиний уніфікований стандарт	Єдиний уніфікований стандарт
Сервіси	Аналоговий стандарт, мовні повідомлення	Цифровий стандарт, підтримка коротких повідомлень (SMS)	WCDMA CDMA2000 UMTS	Велика ємність, IP-орієнтована мережа, підтримка мультимедіа, швидкості до сотень мегабіт на секунду	Велика ємність, IP-орієнтована мережа, підтримка мультимедіа, швидкості до сотень гігабіт на секунду

Рисунок 3.1 Розвиток мереж стільникового зв'язку[36]

Стандарт 5G повинен забезпечити такі характеристики:

- пікова швидкість завантаження даних на одну базову станцію до 20 Гб/с;
- швидкість завантаження даних до 100 Мб / с і вивантаження до 50 Мб/с для одного абонента;
- можливість абонентського пристрою рухатися зі швидкістю до 500 км/г між базовими станціями;

- можливість пристроям перемикатися між режимом заощадження енергії і повністю робочим за 10 мс;
- затримки до 4 мс при сприятливих умовах, і до 1 мс – для спеціалізованих з'єднань;
- поліпшена ефективність використання радіочастотного спектру;
- передача даних зі швидкістю 1 Гб/с в той же час для багатьох користувачів на одному поверсі будівлі;
- можливість роботи до 1 млн пристроїв на 1 км.

5G зробить поштовх до вдосконалення старих та впровадження нових технологій в різних сферах нашого життя, за допомогою впровадження швидкого та безперебійного зв'язку.

Серед цих сфер життя є: медицина, технології, розумний будинок, розумне місто, розваги. [37] Надалі розглянемо більш детально ці сфери життя.

3.2.1 Сектор медицини

Після впровадження технології 5G стане можливим проведення операцій на далекій відстані від фактичного місцезнаходження хворого. При цьому хірург буде відчувати відчувати все, що відбувається в операційній, включаючи тактильні відчуття.(див. рис. 3.2)



Рисунок 3.2 Лікар здійснює віддалено управління апаратом УЗД[37]

У його розпорядженні буде спеціальне обладнання, за допомогою якого він зможе управляти необхідними інструментами і бути присутнім на операції онлайн.

Крім того, 5G допоможе оперативно реагувати на погіршення стану здоров'я хворих через спеціальні датчики, або цілком звичні сьогодні смарт-годинники. Щось подібне вже намагалася зробити Apple з "захистом від падінь" в Apple Watch 4, але на даний момент ця функція без 5G є досить не підготовленою до реального життя.

Завдяки максимальним швидкостями 5G стане можлива швидка розшифровка ДНК. Хоча ця процедура виконується і зараз, вона вимагає пересилки величезних обсягів даних: інформація про геноми однієї людини займає близько 140 гігабайт, відправка яких займе всього одну-дві хвилини.

Якщо людина потрапить в аварію, або у неї станеться серцевий напад, ваш лікар швидко отримає інформацію і відправить карету швидкої допомоги. Завдяки датчикам розташованим у вашому пристрої карета лікарів точно будуть знати ваше місце розташування.

3.2.2 Безпілотні авто та квадрокоптери

В майбутньому 5G дозволить знизити ймовірність ДТП, а також розвинути еру безпілотних автомобілів. Машини будуть набагато чіткіше та швидше реагувати на зміни дорожньої ситуації і оминати більш завантажені вулиці – це дозволить знизити кількість заторів на дорозі.

Безпілотні авто будуть взаємодіяти з камерами, світлофорами, шлагбаумами. Миттєво перевіряти інформацію про стан доріг, зміни погоди.(див. рис. 3.3)

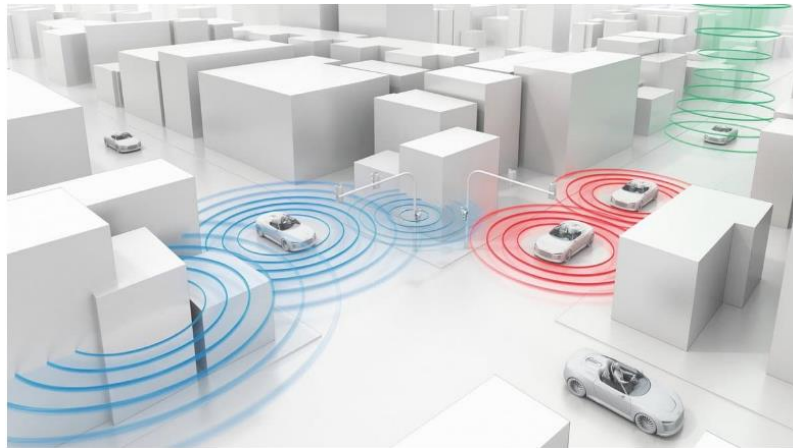


Рисунок 3.3 Принцип роботи безпілотних транспортних засобів[37]

Збільшиться максимальна дальність польоту квадрокоптера і буде обмежуватися тільки ємністю акумулятору. Буде можливе віддалене управління дронами в режимі реального часу. Апарати будуть постійно обмінюватися інформацією один з одним, що також дозволить налагодити їх масове використання без допомоги людини.(див. рис. 3.4)



Рисунок 3.4 Квадрокоптери в розумних містах[37]

Квадрокоптери можна буде використовувати для пошуку людей, що заблукали в важко доступних місцях та в разі необхідності оперативно доставити їм необхідні медикаменти та речі, поки рятувальники зможуть до них дістатися.

3.2.3 Розумні будинки

Через те, що 5G допоможе отримати доступ до мобільного інтернету набагато більшій кількості пристроїв, ніж це може надати зв'язок нинішнього покоління, це допоможе зв'язати між собою всю техніку, яка знаходиться у вашому будинку і навіть за її межами.

Зараз можливо віддалено включити мультиварку або кондиціонер, але це досить дороге задоволення і має певні обмеження. З розвитком 5G все стане дешевше і працювати буде в рази швидше. Вбудовані чіпи не тільки включатимуть техніку, а й будуть слідкувати за технічним станом приладів, це збільшить термін експлуатації та дозволить запобігати раптовим поломкам .

3.3 Висновки до розділу 3

В третьому розділі було розв'язано такі питання:

- Досліджено стан технологій передачі даних на довгі відстані в IoT мережі на основі відомих українських операторів зв'язку, таких як LoRaWAN та NB-IoT .
- Проаналізовано перспективи розвитку IoT на основі найбільш перспективної технології передачі даних 5G. Розглянуто сфери можливого використання технології 5G: сектор медицини, безпілотні авто та розумні будинки.

ВИСНОВКИ

- 1) Розглянуто основні терміни в IoT. Архітектура Інтернет речей складається з чотирьох основних рівнів, таких як: рівень датчиків, мережевого рівня, рівня обробки даних та прикладного рівня. Розглянуто еталонну модель IoT, її основні та додаткові рівні, а також переваги та недоліки IoT мереж.
- 2) Розглянуто основні технології та протоколи передачі даних на довгій дистанції, які входять до складу мереж LPWAN: LoRaWAN, SigFox, NB-IoT, Weightless-P. Здійснено порівняльний аналіз основних характеристик протоколів та технологій передачі даних на довгій відстані таких, як метод модуляції, діапазон частот, швидкість передачі даних, смуга частот, швидкість передачі даних, максимальний час автономної роботи пристроїв, частоти на яких працюють дані технології, рівень безпеки, дальність переді даних.
- 3) Розглянуто основні технології та протоколи передачі даних на короткій відстані, які входять до складу мереж WPAN та WLAN: Z-Wave, RFID, Bluetooth Low Energy та Wi-Fi HaLow. Здійснено порівняльний аналіз основних характеристик протоколів та технологій передачі даних на короткій відстані таких, як смуга частот, швидкість передачі даних, радіус дії, пропускна здатність в каналі, вид модуляції, топологія, безпека.
- 4) Розглянуто топологію, яка використовується для передачі повідомлень в IoT. Здійснено порівняльний аналіз протоколів передачі повідомлень за такими показниками: протокол транспортного рівня, який використовується для передачі повідомлення до користувача IoT, призначення та особливості протоколу, а також операції, які він виконує в мережі IoT.
- 5) Досліджено стан технологій передачі даних на довгій відстані в IoT мережі на основі відомих українських операторів зв'язку, таких як LoRaWAN та NB-IoT.

- 6) Проаналізовано перспективи розвитку IoT на основі найбільш перспективної технології передачі даних 5G. Розглянуто сфери можливого використання технології 5G: сектор медицини, безпілотні авто, квадрокоптери та розумні будинки.

СПИСОК ЛІТЕРАТУРИ

1. Интернет вещей в научных исследованиях // электрон. текст. дані URL:
<https://cyberleninka.ru/article/v/internet-veschey-v-nauchnyh-issledovaniyah> (дата звернення: 01.06.2019)
2. Интернет речей: чи зможе смартфон управляти бізнесом // электрон. текст. дані URL:
<http://persona.pumb.ua/ua/club/digest/detail.php?CODE=internet-veshchey-smozhet-li-smartfon-upravlyat-biznesom> (дата звернення: 01.06.2019)
3. АНАЛИЗ ТРАФИКА УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ // электрон. текст. дані URL:
<https://cyberleninka.ru/article/v/analiz-trafika-ustroystv-interneta-veschey> (дата звернення: 01.06.2019)
4. МСЭ-Т Y.2060 // электрон. текст. дані URL:
<https://www.itu.int/rec/T-REC-Y.2060-201206-I> (дата звернення: 01.06.2019)
5. A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications // электрон. текст. дані URL:
<https://arxiv.org/pdf/1802.02041.pdf> (дата звернення: 01.06.2019)
6. IoT Explained — How Does an IoT System Actually Work? // электрон. текст. дані URL:
<https://medium.com/iotforall/iot-explained-how-does-an-iot-system-actually-work-e90e2c435fe7> (дата звернення: 01.06.2019)
7. The advantages and disadvantages of Internet Of Things // электрон. текст. дані URL:
<https://e27.co/advantages-disadvantages-internet-things-20160615/> (дата звернення: 01.06.2019)

8. The advantages and disadvantages of Internet Of Things (IoT) // електрон. текст. дані URL:
<https://www.linkedin.com/pulse/advantages-disadvantages-internet-things-iot-tommy-quek>(дата звернення: 01.06.2019)
9. ОБЗОР И СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ LPWAN СЕТЕЙ // електрон. текст. дані URL:
www.sut.ru/doci/nauka/review/20164/33-48.pdf (дата звернення: 01.06.2019)
10. История появления технологии LoRa // електрон. текст. дані URL:
<https://nehta.tech/technology/> (дата звернення: 01.06.2019)
11. ЧТО ТАКОЕ LORA? // електрон. текст. дані URL:
<http://lo-ra.ru/lora/> (дата звернення: 01.06.2019)
12. MAC Layer Protocols for Internet of Things: A Survey // електрон. текст. дані URL:
<https://www.mdpi.com/1999-5903/11/1/16/htm> (дата звернення: 01.06.2019)
13. Sigfox Technology // електрон. текст. дані URL:
<https://www.betasolutions.co.nz/Blog/17/Sigfox-Technology-Review>
(дата звернення: 01.06.2019)
14. NB-IoT: как он работает? Часть 1 // електрон. текст. дані URL:
https://m.habr.com/ru/company/ru_mts/blog/430496/ (дата звернення: 01.06.2019)
15. Z-Wave // електрон. текст. дані URL:
<https://ru.wikipedia.org/wiki/Z-Wave> (дата звернення: 01.06.2019)
16. Z-Wave Technical Basics // електрон. текст. дані URL:
<https://www.domotiga.nl/attachments/download/1075/Z-Wave%20Technical%20Basics-small.pdf> (дата звернення: 01.06.2019)
17. Технология NFC — связь на близком расстоянии // електрон. текст. дані URL:

<http://www.russianelectronics.ru/leader-r/review/2187/doc/57689/> (дата звернення: 01.06.2019)

18. Технология NFC принципы работы и преимущества // электрон. текст. дані URL:

<http://www.fotokomok.ru/tehnologiya-nfc-principy-raboty-i-preimushhestva/> (дата звернення: 01.06.2019)

19. RFID-технология // электрон. текст. дані URL:
<https://www.idexpert.ru/technology/121/> (дата звернення: 01.06.2019)

20. RFID-технологии и магнитные метки // электрон. текст. дані URL:
<http://allta.com.ua/what-is-rfid> (дата звернення: 01.06.2019)

21. Bluetooth с низким энергопотреблением // электрон. текст. дані URL:

https://ru.m.wikipedia.org/wiki/Bluetooth_%D1%81_%D0%BD%D0%B8%D0%B7%D0%BA%D0%B8%D0%BC_%D1%8D%D0%BD%D0%B5%D1%80%D0%B3%D0%BE%D0%BF%D0%BE%D1%82%D1%80%D0%B5%D0%B1%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%D0%BC (дата звернення: 01.06.2019)

22. The Basics of Bluetooth Low Energy (BLE) // электрон. текст. дані URL:

<https://www.novelbits.io/basics-bluetooth-low-energy/> (дата звернення: 01.06.2019)

23. ПРИМЕНЕНИЕ BLUETOOTH-ТЕХНОЛОГИИ В ИНТЕРНЕТЕ ВЕЩЕЙ // электрон. текст. дані URL:
<https://cyberleninka.ru/article/v/primenenie-bluetooth-tehnologii-v-internete-veschey> (дата звернення: 01.06.2019)

24. Wi-Fi HaLow (IEEE 802.11ah) — дальнобойное беспроводное подключение с низким энергопотреблением для интернета вещей // электрон. текст. дані URL:

<https://www.ixbt.com/news/2016/01/05/wi-fi-halow-ieee-802-11ah.html> (дата звернення: 01.06.2019)

25. Аналитический обзор протоколов Интернета вещей // электрон. текст. дані URL:
<http://lib.tssonline.ru/articles2/reviews/analiticheskiy-obzor-protokolov-interneta-veschey> (дата звернення: 01.06.2019)
26. What's The Difference Between DDS And AMQP? // электрон. текст. дані URL:
<https://www.electronicdesign.com/embedded/what-s-difference-between-dds-and-amqp> (дата звернення: 01.06.2019)
27. Протоколы «Интернета вещей»: основные сведения // электрон. текст. дані URL:
<http://old.rtsoft.ru/press/articles/detail.php?ID=2718> (дата звернення: 01.06.2019)
28. XMPP // электрон. текст. дані URL:
<https://ru.wikipedia.org/wiki/XMPP> (дата звернення: 01.06.2019)
29. Что такое MQTT и для чего он нужен в IoT? Описание протокола MQTT // электрон. текст. дані URL:
<https://ipc2u.ru/articles/prostye-resheniya/chto-takoe-mqtt/> (дата звернення: 01.06.2019)
30. Протокол MQTT. Особенности, варианты применения, основные процедуры MQTT Protocol. // электрон. текст. дані URL:
<http://www.mka.ru/categories/81/10416/> (дата звернення: 01.06.2019)
31. Технологии для Web-сервисов // электрон. текст. дані URL:
<https://compress.ru/article.aspx?id=10975> (дата звернення: 01.06.2019)
32. Интернет вещей: В Украине построят сети для роботов и датчиков // электрон. текст. дані URL:
<https://biz.liga.net/all/telekom/article/oni-byli-kiborgi-v-ukraine-stoyat-seti-dlya-robotov-i-datchikov> (дата звернення: 01.06.2019)
33. lifecell и IoT Ukraine развернули сеть интернета вещей в трех городах Украины // электрон. текст. дані URL:

<http://mediasat.info/2019/04/16/lifecell-i-iot-ukraine/> (дата звернення: 01.06.2019)

34. Особливості побудови мережі Інтернету речей від lifecell та IoT Ukraine // електрон. текст. дані URL:

<https://www.imena.ua/blog/the-internet-of-things-from-lifecell-and-iot-ukraine/> (дата звернення: 01.06.2019)

35. Що таке 5G та коли технологія з'явиться в Україні // електрон. текст. дані URL:

https://24tv.ua/techno/5g_internet_shho_tse_koli_5g_tehnologiya_bude_v_ukrayini_n1119734 (дата звернення: 01.06.2019)

36. Україну чекає "революція" з інтернетом і зв'язком: що зміниться // електрон. текст. дані URL:

<https://www.obozrevatel.com/ukr/tech/5g-v-ukraini-perevagi-ta-termini-vvedennya.htm> (дата звернення: 01.06.2019)

37. В КАКИХ СФЕРАХ БУДЕТ ИСПОЛЬЗОВАТЬСЯ 5G // електрон. текст. дані URL:

<https://www.computerra.ru/233168/v-kakih-sferah-budet-ispolzovatsya-5g/> (дата звернення: 01.06.2019)

38. Внедрение RFID технологии для автоматизации склада и проведения инвентаризации // електрон. текст. дані URL:

<https://1cab.ru/ab/news/VnedrenieRFIDtekhnologiiidlyaavtomatizatsiisklaidaiprovedeniyainventarizatsii/> (дата звернення: 01.06.2019)